NEW SOLUTIONS TO DELSARTE'S DUAL LINEAR PROGRAMS

ANDRÉ CHAILLOUX AND THOMAS DEBRIS–ALAZARD

ABSTRACT. Understanding the maximum size of a code with a given minimum distance is a major question in computer science and discrete mathematics. The most fruitful approach for finding asymptotic bounds on such codes is by using Delsarte's theory of association schemes. With this approach, Delsarte constructs a linear program such that its maximum value is an upper bound on the maximum size of a code with a given minimum distance. Bounding this value can be done by finding solutions to the corresponding dual linear program. Delsarte's theory is very general and goes way beyond binary codes.

In this work, we provide universal bounds in the framework of association schemes that generalize the Hamming bound and the Elias-Bassalygo bound, which can be applied to any association scheme constructed from a distance function. These bounds are obtained by constructing new solutions to Delsartes dual linear program. We instantiate these results and we recover known bounds for q-ary codes and for constant-weight binary codes but which didn't come from the linear program method. Our other contribution is to recover, for essentially any Q-polynomial scheme, MRRW-type solutions to Delsarte's dual linear program which are inspired by the Laplacian approach of Friedman and Tillich instead of using the Christoffel-Darboux formulas. We show in particular how the second linear programming bound can be interpreted in this framework.

1. INTRODUCTION

Let τ_{H} denote the Hamming distance. For a subset of the boolean cube, *i.e.,* a binary code $\mathcal{C} \subseteq \mathbb{F}_2^n$, its minimum distance is $d_{\min}^{\mathrm{H}}(\mathcal{C}) = \min\{\tau_{\mathrm{H}}(\mathbf{c}-\mathbf{c}') : \mathbf{c},\mathbf{c}' \in \mathcal{C} \text{ with } \mathbf{c} \neq \mathbf{c}'\}$. We define $A(n,d)$ as being the maximum size of a binary code with some fixed minimum distance, *i.e.,*

$$A(n,d) \overset{\text{def}}{=} \max\left\{|\mathcal{C}| : \mathcal{C} \subseteq \mathbb{F}_2^n,\ d_{\min}^{\mathrm{H}}(\mathcal{C}) = d\right\}.$$

We are interested in the maximum asymptotic rate of binary codes with a certain (relative) minimum distance $\delta \in [0,1]$, *i.e.,*

$$R(\delta) \overset{\text{def}}{=} \overline{\lim_{n\to\infty}} \frac{1}{n} \log_2 A(n, \lfloor \delta n \rfloor).$$

There are many reasons why one can be interested in this quantity. Constructing binary codes with large minimum distance is studied since the seminal work of Shannon [Sha48]. Understanding $R(\delta)$ has important consequences for telecommunications, in particular to provide lower bounds on the probability of undetected error and for finding optimal codes for error detection over the binary-symmetric channel [SGB67]. Moreover, it is a fundamental question in discrete mathematics and it is strongly related to sphere packings in $\mathbb{R}^n$ [KL78, CE03]. Finally, the fact that the best bounds on $R(\delta)$ were found in the late 1970's, and are quite far from what we expect, makes it a particularly interesting question for mathematicians and computer scientists.

Another important question is to provide bounds on the size of constant-weight codes with a certain minimum distance. These codes are subsets of $\mathcal{S}_a^{n,2} \overset{\text{def}}{=} \{\mathbf{x} \in \mathbb{F}_2^n : \tau_h(\mathbf{x}, \mathbf{0}) = a\}$. We are interested in the following quantity[(1)],

$$A(n,d,a) \overset{\text{def}}{=} \max\left\{|\mathcal{C}| : \mathcal{C} \subseteq \mathcal{S}_a^{n,2},\ d_{\min}^{\mathrm{H}}(\mathcal{C}) = d\right\}.$$

Again, we define the asymptotic rate of constant-weight codes of relative weight α with a certain relative minimum distance δ,

$$R(\delta,\alpha) = \overline{\lim_{n\to+\infty}} \frac{1}{n}\log_2 A(n,\lfloor\delta n\rfloor,\lfloor\alpha n\rfloor).$$

Studying this quantity is interesting for its own sake but it is of additional importance because it can be used to obtain bounds on $R(\delta)$ thanks to the Elias-Bassalygo relation,

$$\forall \alpha \in \left[0,\frac{1}{2}\right], \quad R(\delta) \leq 1 - h(\alpha) + R(\delta,\alpha) \tag{1}$$

where $h(x) \overset{\text{def}}{=} -x\log_2 x - (1-x)\log_2(1-x)$ denotes the binary entropy.

1.1. An Overview of Some Different Bounds and Linear Programming Bounds.

The best lower bound on $R(\delta)$ is the so-called Gilbert-Varshamov bound [Gil52, Var57],

$$R(\delta) \geq R_{\mathrm{GV}}(\delta) \overset{\text{def}}{=} 1 - h(\delta).$$

It turns out that this bound corresponds to the minimum distance that is obtained by choosing a random linear code of the appropriate size. We expect this bound to be tight even though in the q-ary setting (when working in $\mathbb{F}_q^n$), there are codes that have a better minimum distance than random linear codes of the same size as soon as $q = p^2$ with $p \geq 7$ [TVZ82] so the whole picture is not entirely clear.

On the other hand, there are various upper bounds on $R(\delta)$. The simplest known upper bound is the combinatorial Hamming bound. This bound was improved independently by Elias (attributed to Elias in [SGB67]) and Bassalygo [Bas65] also by using combinatorial arguments. These bounds are the following,

$$R(\delta) \leq R_{\mathrm{Hamm}}(\delta) \overset{\text{def}}{=} 1 - h\left(\frac{\delta}{2}\right),$$
$$R(\delta) \leq R_{\mathrm{EB}}(\delta) \overset{\text{def}}{=} 1 - h\left(\frac{1}{2} - \frac{1}{2}\sqrt{1-2\delta}\right).$$

The question of finding codes with minimum distance d can be generalized to the following question: given a set X and some distance function τ over X, what is the maximum size of a subset $\mathcal{C} \subseteq \mathsf{X}$ such that each pair of distinct point of $\mathcal{C}$ have distance at least d? Delsarte introduced the important notion of association schemes [Del73] that can in particular help solving this question. More precisely, if (X,τ) satisfies certain conditions, then using the theory of association schemes, Delsarte shows how to construct a linear program such that its maximum value will be a bound on the maximum size of $\mathcal{C}$ with minimum distance at least d. An overview of Delsarte's theory can be found in [DL98].

When instantiated in the boolean cube, this linear program involves Krawtchouk polynomials and MacWilliams identities. Its maximum objective $A_{\mathrm{LP}}(n,d)$ satisfies $A(n,d) \leq A_{\mathrm{LP}}(n,d)$. Then, it is possible to deduce upper bounds on $A_{\mathrm{LP}}(n,d)$ by finding solutions to the associated dual linear program. Again, as we are interested in asymptotic upper bounds, we write,

$$R_{\mathrm{LP}}(\delta) \overset{\text{def}}{=} \overline{\lim_{n\to+\infty}} \frac{1}{n}\log_2 A_{\mathrm{LP}}(n,\lfloor\delta n\rfloor).$$

[(1)] The number of arguments of $A(\cdot)$ will make it clear whether we talk about bounds on general codes or on constant-weight codes.

Using Delsarte's approach, McEliece, Rodemich, Rumsey and Welch [MRRW77] proved what is now called the first linear programming bound,

$$R(\delta) \le R_{\mathrm{LP}}(\delta) \le R_{\mathrm{MRRW1}}(\delta) \overset{\mathrm{def}}{=} h\left(\frac{1}{2} - \frac{1}{2}\sqrt{\delta(1-\delta)}\right).$$

It turns out that Delsarte's linear program approach can also be used to obtain bounds on the size of constant-weight codes with a certain minimum distance. It yields a linear program involving dual Hahn polynomials such that its optimum $A_{\mathrm{LP}}(n,d,a)$ satisfies[(2)] $A(n,d,a) \le A_{\mathrm{LP}}\left(n, \lfloor \frac{d}{2} \rfloor, a\right)$. We denote the asymptotic value of this linear program,

$$R_{\mathrm{LP}}(\delta,\alpha) = \overline{\lim_{n\to\infty}} \frac{1}{n} \log_2 A_{\mathrm{LP}}(n, \lfloor \delta n \rfloor, \lfloor \alpha n \rfloor).$$

Again, by finding solutions to the associated dual linear program, it was shown in [MRRW77] that,

$$(2) \qquad R(\alpha,\delta) \le R_{\mathrm{LP}}\left(\alpha, \frac{\delta}{2}\right) \le R_{\mathrm{MRRW}}(\alpha,\delta) \overset{\mathrm{def}}{=} \frac{1}{2}\left(1 - \sqrt{1 - 4\left(\sqrt{\alpha(1-\alpha) - \delta(1-\delta)} - \delta\right)^2}\right).$$

This bound is of particular importance because it can be combined with the Elias-Bassalygo relation (Equation (1)) to prove the so-called second linear programming bound,

$$R(\delta) \le R_{\mathrm{MRRW2}}(\delta) \overset{\mathrm{def}}{=} \max_{0 \le \alpha \le \frac{1}{2}} \{1 - h(\alpha) + R_{\mathrm{MRRW}}(\alpha,\delta)\}$$

This bound is, for the last 47 years, the best known upper bound on $R(\delta)$ for any δ, but it is quite far from the lower bound $R_{\mathrm{GV}}(\delta)$. Note that even if there were some improvements on $R(\delta,\alpha)$ for some parameters (see [Sam01] for example), these do not yield any improvements on $R(\delta)$ by using Equation (1). Surprisingly, Rodemich proved [Rod80] (see also [Del94, Sam01, AB06]) a lifting theorem which shows how to construct solutions to Delsarte's dual linear program on the boolean cube from a solution to the dual linear program for constant-weight codes. In particular, Rodemich has shown how to use Equation (2) to prove,

$$R_{\mathrm{LP}}(\delta) \le R_{\mathrm{MRRW2}}(\delta)$$

without using the Elias-Bassalygo relation. In other words, the best (current) solution of the linear program in the boolean cube leads to the second linear programming bound. An overview of these different bounds on $R(\delta)$ is depicted in Figure 1.

While [MRRW77] restricts its bounds to the binary case, an interesting question is also to provide bounds on the maximal size $A^{(q)}(n,d)$ of a code in $\mathbb{F}_q^n$ of minimum distance d and on the asymptotic rate $R^{(q)}(\delta) = \overline{\lim_{n\to+\infty}} \frac{1}{n} \log_q A^{(q)}(n, \lfloor \delta n \rfloor)$ of codes in $\mathbb{F}_q^n$, with $q > 2$ a prime power, as function of their relative minimum distance δ. Unfortunately, Hamming spheres in $\mathbb{F}_q^n$, in which constant-weight codes are embedded, do not yield association schemes and Delsarte's approach fails to provide a linear program. Therefore there is no equivalent to the second linear programming bound and an equivalent to Rodemich's lifting theorem does not exist. However, other bounds such as the first linear programming bound can easily be extended to the q-ary case [DL98, §F.],

$$R^{(q)}(\delta) \le R^{(q)}_{\mathrm{LP}}(\delta) \le R^{(q)}_{\mathrm{MRRW1}}(\delta) \overset{\mathrm{def}}{=} h_q\left(\gamma_q(\delta)\right) \text{ where}$$

$$h_q(x) \overset{\mathrm{def}}{=} -(1-x)\log_q(1-x) - x\log_q\left(\frac{x}{q-1}\right) \quad , \quad \gamma_q(\delta) \overset{\mathrm{def}}{=} \frac{1}{q}\left(q - 1 - (q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)}\right).$$

Furthermore, Hamming and Elias-Bassalygo bounds are also known in this setting by using the same combinatorial arguments. For instance, the asymptotic Elias-Bassalygo bound in given in

[(2)] The factor two in the distance comes from the fact that the corresponding association scheme uses as its distance function $\tau_{\mathrm{H}}/2$.

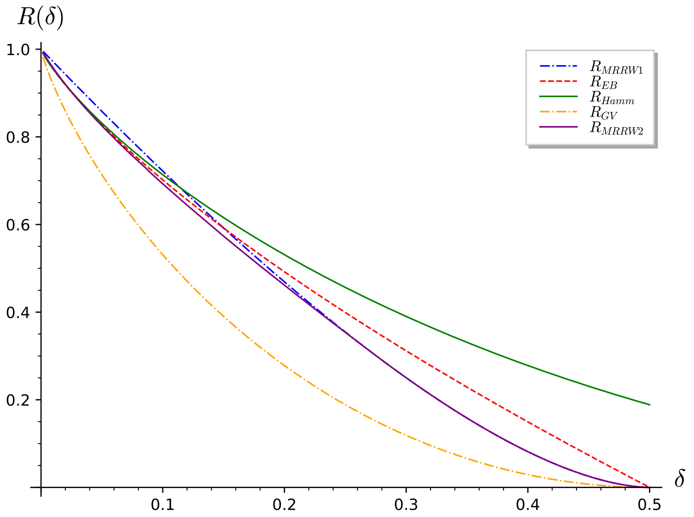

Figure 1. Known upper bounds and the Gilbert-Varshamov lower bound on the asymptotic rate of binary codes $R(\delta)$ as function of their relative minimum distance δ.

the q-ary case by,

$$R^{(q)}(\delta) \leq R_{\mathrm{EB}}^{(q)} \overset{\text{def}}{=} 1 - h_q\left(J_q(\delta)\right) \qquad \text{where} \;\; J_q(\delta) \overset{\text{def}}{=} \left(1 - \frac{1}{q}\right) \cdot \left(1 - \sqrt{1 - \frac{q\delta}{(q-1)}}\right).$$

1.2. **Understanding the Limits of the Linear Programming Approach.** Delsarte's linear program approach is currently the most efficient one to provide bounds on $R(\delta)$. A natural question is therefore whether the second linear programming bound is the best one that can be achieved with this method. Also, there has recently been proposals for a hierarchy of linear programs involving a generalized Delsarte's linear program on the boolean cube that give the real value $R(\delta)$ when going far enough in the hierarchy [CJJ22, LL23, CJJ23]. Unfortunately, these linear programs are currently too complicated to find new bounds and understanding solutions of Delsarte's linear program could be useful for finding new solutions to these more general linear programs.

More concretely, what do we know about $R_{\mathrm{LP}}(\delta)$? The best upper bound is $R_{\mathrm{LP}}(\delta) \leq R_{\mathrm{MRRW2}}(\delta)$ using the MRRW bound for constant-weight codes and Rodemich's lifting theorem. On the other hand, regarding lower bounds, the following bounds are known, which were proven respectively by Samorodnitsky [Sam01] and by Navon and Samorodnitsky [NS05],

$$R_{\mathrm{LP}}(\delta) \geq R_{\mathrm{LP}}^{\mathrm{LWB1}} \overset{\text{def}}{=} \frac{1}{2}\left(R_{\mathrm{GV}}(\delta) + R_{\mathrm{MRRW1}}(\delta)\right),$$

$$R_{\mathrm{LP}}(\delta) \geq R_{\mathrm{LP}}^{\mathrm{LWB2}} \overset{\text{def}}{=} \frac{1}{2} h\left(1 - 2\sqrt{\delta(1-\delta)}\right).$$

In the attempt to understand the tightness of $R_{\mathrm{LP}}^{\mathrm{LWB1}}$, Barg and Jaffe [BJ99] performed numerical simulations for $A_{\mathrm{LP}}(n,d)$ with $n = 1000$. Their numerical simulations have shown that $R_{\mathrm{LP}}(\delta)$ is actually likely to be close to $R_{\mathrm{MRRW2}}(\delta)$. The above two lower bounds and this upper bound are depicted in Figure 2.

In the case of constant-weight codes, the problem was less studied and the best bound is, to the best of our knowledge, $R_{\mathrm{LP}}(\delta, \alpha) \leq R_{\mathrm{MRRW}}(\delta, \alpha)$.

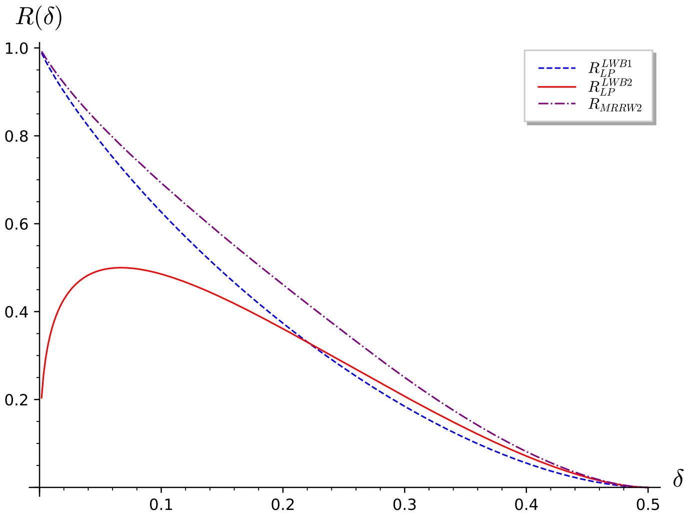

Figure 2. Best upper bound $R_{\mathrm{MRRW2}}(\delta)$ on Delsarte's linear program instantiated in the boolean cube and known lower bounds on this program as function of the relative minimum distance δ.

1.3. **The Laplacian Technique.** The linear programming technique seems to have intrinsic limitations so it is important to consider other approaches. In this attempt, an extensive line of work started with the approach of Friedman and Tillich [FT05] which relied on graph theory and Fourier analysis over the Hamming cube. Roughly speaking, [FT05] study the following: given a *linear* code $\mathcal{C}$, start from a random element of its dual and then walk on the Hamming cube according to some distribution f. Then, it turns out than an upper bound over the size of $\mathcal{C}$ can be found using a function satisfying

$$\mathbf{1}_{\{1\}} \star f \geq \lambda f. \tag{3}$$

for some real λ, where $\mathbf{1}_{\{1\}}$ denotes the indicator function of words with Hamming weight 1 and $\star$ is the canonical convolution product. The value λ is related to the minimum distance of $\mathcal{C}$ while the obtained upper bound on $\mathcal{C}$ can be expressed as a function of the range of f. In short, Friedman and Tillich find a function f with small range such that Equation (3) is satisfied for a large λ. They recover the first linear programming bound with this approach seemingly orthogonal to Delsarte's linear program. Notice that the operation $\mathbf{1}_{\{1\}} \star f$ consists in performing an extra random step of Hamming distance 1 after applying f. Because the operation $\mathbf{1}_{\{1\}} \star f$ is closely related to the Laplacian of f, we call this approach the Laplacian technique.

Several other works [Sam01, NS05] have followed the Laplacian technique by using Equation (3) in a crucial way. It has been shown among others that it can also be interpreted in terms of covering radius of the dual graph and can even be extended to non-linear codes [NS07]. However, these methods are all tailored for the first linear programming by using Fourier analysis in the boolean cube. It is an open question (see [NS07] for instance) whether these methods can be adapted to the second linear programming bound.

1.4. **Contributions.** Our first contribution is to give explicit solutions to Delsarte's dual linear programs that achieve a generalized Hamming bound which we also improve to a generalized Elias-Bassalygo bound. This result is very general and can be applied to any P-polynomial association scheme under mild conditions.

In the case of the boolean cube, we find solutions to the dual linear program of Delsarte (explaining our expression of "generalized" Elias-Bassalygo bound) that give,

$$R_{\mathrm{LP}}(\delta) \le R_{\mathrm{EB}}(\delta).$$

This shows a simple example of Delsarte's linear program solutions on the Hamming cube which are very different from the MRRW solutions. Furthermore, it achieves a better bound than $R_{\mathrm{MRRW1}}(\delta)$ for small values of δ without the use of Rodemich's lifting theorem. These solutions also show how to overcome some of the difficulties presented in [Sam23a] on beating the first linear programming bound with this approach.

With out framework, we can actually extend this to the q-ary setting, *i.e.,* when considering codes in $\mathbb{F}_q^n$. In this case, Delsarte's framework still applies and we obtain,

$$R_{\mathrm{LP}}^{(q)}(\delta) \le R_{\mathrm{EB}}^{(q)}(\delta).$$

One can then show that for any q, there exists a δ_0 such that,

$$\forall \delta \in (0,\delta_0), \quad R_{\mathrm{EB}}^{(q)}(\delta) < R_{\mathrm{MRRW1}}^{(q)}(\delta).$$

This gives, to the best of our knowledge, new solutions to the q-ary dual linear program which on the first linear programming bound for small relative minimum distance δ.

In the case of constant-weight codes, we only have results for the binary case since this is the only case where there is an associations scheme structure. We derive from our new solution to the dual linear program the following bound,

$$R_{\mathrm{LP}}(\delta,\alpha) \le R_{\mathrm{EB}}(\delta,\alpha) \overset{\mathrm{def}}{=} h(\alpha) - \alpha h\left(\frac{x}{\alpha}\right) - (1-\alpha) h\left(\frac{x}{1-\alpha}\right) \quad \text{with } x \overset{\mathrm{def}}{=} \alpha(1-\alpha)\left(1 - \sqrt{\frac{\delta}{\alpha(1-\alpha)}}\right).$$

Again, it can be verified that for any $\alpha \in \left(0,\frac{1}{2}\right)$, $R_{\mathrm{EB}}(\delta,\alpha) < R_{\mathrm{MRRW}}(\delta,\alpha)$ for δ small enough which again gives simple and sometimes better alternative solutions to this linear program.

Our second contribution is to find explicit MRRW type solutions to Delsarte's linear program for essentially any Q-polynomial scheme. We rely on functions f satisfying,

$$\mathbf{1}_{\{1\}} \circledast f \ge \lambda f \tag{4}$$

where $\circledast$ is not the canonical convolution of the association scheme derived from its underlying adjacency matrices and P-polynomials, but the convolution product derived from Q-polynomials. This can be seen as a direct "dual" generalization of Friedman and Tillich' approach. We then show that the function $g = \mathbf{1}_{\{1\}} \circledast f \circledast f - (\lambda-1)(f \circledast f)$ gives a solution to the dual linear program. This is a generalization of the observation of Samorodnitsky [Sam23b]. We also give an explicit construction for "good" functions f satisfying Equation (4), that depends only on the Q-polynomials of the association scheme, generalizing [LL22].

When correctly instantiated to Hamming spheres, we recover $R_{\mathrm{MRRW}}(\delta,\alpha)$ so this technique can be seen in some sense as a generalization of the Laplacian technique to the second linear programming bound. One has to be careful though, because we work with the convolution product in the Q-polynomial world. We somehow need to do the "in reverse" argument of the Laplace technique and use a "dual" Laplacian technique. While this is very well defined in the framework of association schemes, we don't know how to interpret the operation $\mathbf{1}_{\{1\}} \circledast f$ in terms of random walks on the associated inherited graph from spheres or in terms of a covering radius in the dual space. The fact that we require the Q-polynomial convolution for this generalization rather illustrates the difficulties in finding such interpretations.

Because our results are meant to be as general as possible, we rely on the full machinery of association schemes. We therefore present an extensive introduction to Delsarte's theory of association schemes before proving our results.

2. Notation and Preliminaries on Association Schemes

Basic Notation. The notation $x \overset{\text{def}}{=} y$ means that x is being defined as equal to y. Given a set $\mathcal{S}$, its indicator function will be denoted $\mathbf{1}_{\mathcal{S}}$. For a finite set $\mathcal{S}$, we will denote by $|\mathcal{S}|$ its cardinality. Let $[\![a,b]\!]$ be the set of integers $\{a, a+1, \dots, b\}$. We use the Kronecker delta notation $\delta_i^j = 1$ if $i = j$ and $\delta_i^j = 0$ otherwise.

Matrices are denoted in bold capital letters such as $\mathbf{A}$. For a finite set $\mathcal{S}$, let $\mathbb{C}(\mathcal{S}^2)$ be the set of square matrices of order $|\mathcal{S}|$ and whose coefficients belong to $\mathbb{C}$. We will use the standard inner product on $\mathbb{C}\left(\mathcal{S}^2\right)$, *i.e.,* for $\mathbf{A}, \mathbf{B} \in \mathbb{C}\left(\mathcal{S}^2\right)$,

$$\langle \mathbf{A} | \mathbf{B} \rangle \overset{\text{def}}{=} \operatorname{tr}\left(\mathbf{A}\mathbf{B}^\dagger\right) \quad , \quad \|\mathbf{A}\| \overset{\text{def}}{=} \sqrt{\langle \mathbf{A} | \mathbf{A} \rangle}$$

where $\mathbf{B}^\dagger$ denotes the conjugate transpose of $\mathbf{B}$. For any fixed order over $\mathcal{S}$ and $x, y \in \mathcal{S}$, we write $\mathbf{A}(x,y)$ to denote the coefficient of $\mathbf{A}$ at row x and column y.

Our aim now is to present needed pre-requisites about association schemes. Almost all proofs are omitted. They can be found in the classical literature about association schemes like [Del73, BI84, DL98]. For the sake of completeness, we prove in Appendix A all the claimed results.

2.1. Equipartition Property and Association Schemes.

Let X be a finite set of "points" with $|\mathsf{X}| \geq 2$ and let $\tau : \mathsf{X}^2 \longrightarrow [\![0,n]\!]$ be a distance function. Given (X, τ, n), we will consider the following adjacency matrices $\mathbf{D}_i \in \mathbb{C}(\mathsf{X}^2)$ for $i \in [\![0,n]\!]$,

$$\forall x, y \in \mathsf{X}, \quad \mathbf{D}_i(x,y) \overset{\text{def}}{=} \begin{cases} 1 \text{ if } \tau(x,y) = 1 \\ 0 \text{ otherwise} \end{cases}.$$

Distance induced association schemes are triplets (X, τ, n) satisfying the following properties.

Definition 1 (Equipartition Property and Non-Degenerate Triplets)**.** *(X, τ, n) is said to satisfy the equipartition property if for each $i, j, k \in [\![0,n]\!]$, there exists a nonnegative integer $p_{i,j}^k$ such that,*

$$\forall x, z \in \mathsf{X} \textit{ such that } \tau(x,z) = k, \quad |\{y \in \mathsf{X} : \tau(x,y) = i \textit{ and } \tau(y,z) = j\}| = p_{i,j}^k.$$

Furthermore, a triplet (X, τ, n) satisfying the equipartition property is said to be non-degenerate if $p_{1,k}^{k+1} \neq 0$ for all $k \in [\![0, n-1]\!]$.

The equipartition property ensures that the complex vector space generated by the adjacency matrices $\mathbf{D}_i$ is closed under matrix multiplication, *i.e.,* it forms an associative algebra.

Proposition 1. *Let (X, τ, n) satisfying the equipartition property and let $(\mathbf{D}_i)_{i \in [\![0,n]\!]}$ denote the associated adjacency matrices. We have,*

$$\forall i, j \in [\![0,n]\!], \quad \mathbf{D}_i \cdot \mathbf{D}_j = \sum_{k \in [\![0,n]\!]} p_{i,j}^k \mathbf{D}_k.$$

The above proposition is extremely powerful, it shows that the vector space generated by the $\mathbf{D}_i$ inherits a lot of structure. In particular, by the symmetry of the distance τ, the $p_{i,j}^k$ verify,

$$\forall i, j, k \in [\![0,n]\!], \quad p_{i,j}^k = p_{j,i}^k.$$

Therefore, it is readily seen that the complex vector space generated by the adjacency matrices $\mathbf{D}_i$ is an associative algebra which is commutative. Furthermore, the fact that the $p_{i,j}^k$ are defined via the distance τ implies another strong property that will be useful:

$$p_{i,j}^k = 0 \text{ if } k > i + j, \text{ or } |j - i| > k \text{ or as soon as } i, j, k > n. \tag{5}$$

We are now ready to properly define distance induced association schemes.

Definition 2. *A distance induced association scheme is a triplet* (X, τ, n) *where* X *is a finite set,* $\tau : \mathsf{X}^2 \longrightarrow [\![0, n]\!]$ *is a distance and* (X, τ, n) *satisfies the equipartition property and is non-degenerate.*

Remark 1. *General association schemes are defined via a collection of some relations* $(\mathcal{R}_i)_{i \in [\![0,n]\!]}$ *over* X^2*. Our definition restricts (which is enough for our purpose) to the case where the* $\mathcal{R}_i$ *are defined via* $(x, y) \in \mathcal{R}_i$ *if and only if* $\tau(x, y) = i$*.*

Remark 2. *Association schemes that satisfy Equation (5) are called P-polynomial association schemes. Any distance induced association scheme is P-polynomial. Conversely, for any P-polynomial association scheme, one can construct a distance function* τ *such that it is distance induced with respect to* τ [Del73, §5.2]*. Also, P-polynomial schemes satisfy the 3-term relation,*

$$\mathbf{D}_1 \mathbf{D}_j = p_{1,j}^{j-1} \mathbf{D}_{j-1} + p_{1,j}^{j} \mathbf{D}_j + p_{1,j}^{j+1} \mathbf{D}_{j+1},$$

which is a key-equation.

The most common association schemes (and the ones that we will consider) are,

- **The Hamming scheme:** X is the hypercube $\mathbb{F}_q^n$ endowed with Hamming metric,
$$\forall \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^n, \quad \tau_{\mathrm{H}}(\mathbf{x}, \mathbf{y}) \overset{\text{def}}{=} |\{i \in [\![1, n]\!] : x_i \neq y_i\}|.$$
- **The Johnson scheme:** given some $a \in [\![0, n]\!]$, $\mathsf{X} = \mathcal{S}_a^{n,2} = \{\mathbf{x} \in \mathbb{F}_2^n : \tau_{\mathrm{H}}(\mathbf{x}, \mathbf{0}) = a\}$ is the Hamming sphere of radius a in the Hamming cube. The association scheme $(\mathsf{X}, \tau_{\mathrm{J}}, a)$ is then defined with[(3)] $\tau_{\mathrm{J}} \overset{\text{def}}{=} \tau_{\mathrm{H}}/2$.

2.2. Fundamental Parameters of Association Schemes.

Let (X, τ, n) be a distance induced association scheme. The corresponding matrices $\mathbf{D}_i$ are real and symmetric. Moreover, from Proposition 1 one can show that each $\mathbf{D}_i$ has $n + 1$ distinct eigenvalues and that they share the same eigenspaces. Let $\mathbf{E}_0, \dots, \mathbf{E}_n$ be the projectors on these eigenspaces.

One can prove that there exists an ordering on the matrices $(\mathbf{E}_i)_{i \in [\![0,n]\!]}$ such that,

$$\mathbf{E}_0 = \frac{1}{|\mathsf{X}|} \sum_{i \in [\![0,n]\!]} \mathbf{D}_i = \frac{1}{|\mathsf{X}|} \cdot \mathbf{J} \quad \text{where } \mathbf{J} \text{ is the full-one matrix.}$$

The fundamental parameters of an association scheme are defined with respect to an ordering of the matrices $\mathbf{E}_0, \dots, \mathbf{E}_n$. When we refer to an ordering $\mathbf{E}_0, \dots, \mathbf{E}_n$, we assume from now on that it satisfies $\mathbf{E}_0 = \frac{1}{|\mathsf{X}|} \cdot \mathbf{J}$.

Definition 3 (p-numbers)**.** *Let* (X, τ, n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0, \dots, \mathbf{E}_n$*. Its underlying p-numbers* $p_i(j)$ *are defined as,*

$$\forall i \in [\![0, n]\!], \quad \mathbf{D}_i = \sum_{j \in [\![0,n]\!]} p_i(j) \mathbf{E}_j.$$

Let us now introduce the norms (with a normalization) of these matrices $\mathbf{D}_i$ and $\mathbf{E}_j$.

Definition 4. *Let* (X, τ, n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0, \dots, \mathbf{E}_n$*, we define,*

$$\forall i \in [\![0, n]\!], \quad v_i \overset{\text{def}}{=} \frac{\|\mathbf{D}_i\|^2}{|\mathsf{X}|} \quad \text{and} \quad m_i \overset{\text{def}}{=} \|\mathbf{E}_i\|^2 = \operatorname{rank}(\mathbf{E}_i).$$

[(3)] One can check that for any $\mathbf{x}, \mathbf{y} \in \mathcal{S}_a^{n,2}$, $\tau_{\mathrm{H}}(\mathbf{x}, \mathbf{y})$ is even hence $\tau_{\mathrm{J}}(\mathbf{x}, \mathbf{y})$ is an integer.

The v_i (*resp.* m_i) are called the valencies (*resp.* multiplicities) of the association scheme. From Definition (1), one can obtain the following relation,

$$\forall i \in [\![0,n]\!], \quad v_i = p_{i,i}^0. \tag{6}$$

Matrices $(\mathbf{D}_i)_{i\in[\![0,n]\!]}$ and $(\mathbf{E}_i)_{i\in[\![0,n]\!]}$ generate the same Hilbert space which enables to define the q-numbers, an analogue of the p-numbers where the $\mathbf{E}_i$ and $\mathbf{D}_i$ are interchanged.

Definition 5 (q-numbers)**.** *Let* (X,τ,n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0,\dots,\mathbf{E}_n$*. Its underlying* q*-numbers* $q_i(j)$ *are defined from the expansion of the orthogonal projectors* $\mathbf{E}_i$ *in the basis of adjacency matrices* $(\mathbf{D}_j)_{j\in[\![0,n]\!]}$*, i.e.,*

$$\forall i \in [\![0,n]\!], \quad \mathbf{E}_i = \frac{1}{|\mathsf{X}|}\sum_{j\in[\![0,n]\!]} q_i(j)\mathbf{D}_j.$$

Notice that the p and q-numbers are real by symmetry of the $\mathbf{D}_i$, $\mathbf{E}_j$ and unicity of the decomposition in theses bases. Furthermore, from the definition of $\mathbf{E}_0$ as $1/|\mathsf{X}|\sum_{i\in[\![0,n]\!]}\mathbf{D}_i$ and the fact that $\mathbf{D}_0 = \mathbf{Id} = \sum_{i\in[\![0,n]\!]}\mathbf{E}_i$, we deduce that,

$$\forall j \in [\![0,n]\!], \quad q_0(j) = 1 \quad , \quad p_0(j) = 1. \tag{7}$$

One can show that the matrices $(\mathbf{D}_i)_{i\in[\![0,n]\!]}$ are pairwise orthogonal with respect to the inner product on matrices. Similarly the matrices $(\mathbf{E}_i)_{i\in[\![0,n]\!]}$ are pairwise orthogonal. This allows to show a strong relation between the p and q-numbers.

Proposition 2. *Let* (X,τ,n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0,\dots,\mathbf{E}_n$*.*

$$\forall i,j \in [\![0,n]\!], \quad m_j p_i(j) = v_i q_j(i).$$

The above relation is the key to prove many formulas involving p and q-numbers. In particular, using that q_0, p_0 are the constant functions equal to 1 by Equation (7), we get $m_0 = \|\mathbf{E}_0\|^2 = 1$, $v_0 = \|\mathbf{D}_0\|^2/|\mathsf{X}| = 1$ and finally,

$$\forall i \in [\![0,n]\!], \quad p_i(0) = v_i \quad , \quad q_i(0) = m_i. \tag{8}$$

2.3. Algebra Structure for Pointwise Multiplication and Q-Polynomial Schemes.

We have deduced from Proposition 1 that the vector space $\mathcal{H}$ generated by the $\mathbf{D}_i$ is closed for the standard matrix-product: it is an algebra. It is also closed under the pointwise multiplication $(\mathbf{M},\mathbf{N}) \mapsto \mathbf{M}\circ\mathbf{N}$ be defined as,

$$\mathbf{M}\circ\mathbf{N}(x,y) \stackrel{\text{def}}{=} \mathbf{M}(x,y)\mathbf{N}(x,y).$$

Indeed the $\mathbf{D}_i$ verify $\mathbf{D}_i\circ\mathbf{D}_j = \delta_i^j\cdot\mathbf{D}_i$. But $\mathcal{H}$ is also generated by the $\mathbf{E}_i$ showing that we can define an equivalent of the $p_{i,j}^k$ (regarding Proposition 1): the $q_{i,j}^k$.

Definition 6. *Let* (X,τ,n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0,\dots,\mathbf{E}_n$*. The underlying Krein parameters* $q_{i,j}^k$ *are defined from the expansion of* $|\mathsf{X}|\cdot\mathbf{E}_i\circ\mathbf{E}_j$ *in the basis* $(\mathbf{E}_k)_{k\in[\![0,n]\!]}$*, i.e.,*

$$\forall i,j \in [\![0,n]\!], \quad |\mathsf{X}|\cdot\mathbf{E}_i\circ\mathbf{E}_j = \sum_{k\in[\![0,n]\!]} q_{i,j}^k\mathbf{E}_k.$$

The Krein parameters enjoy many interesting properties. For instance, they verify the following relations,

$$\forall x \in [\![0,n]\!], \quad q_{x,x}^0 = m_x > 0, \tag{9}$$

$$\forall x \in [\![0,n]\!], \quad \sum_{y\in[\![0,n]\!]} q_{y,1}^x = q_1(0), \tag{10}$$

$$\forall x, y \in [\![0,n]\!], \quad m_x \cdot q_{y,1}^{x} = m_y \cdot q_{x,1}^{y}. \tag{11}$$

But most importantly, Krein parameters are nonnegative.

Proposition 3. $\forall i,j,k \in [\![0,n]\!], \quad q_{i,j}^{k} \geq 0.$

Krein parameters also appear when considering the product of q-numbers.

Proposition 4. $\forall i,k,\ell \in [\![0,n]\!], \quad q_k(i) q_\ell(i) = \sum_{m \in [\![0,n]\!]} q_{k,\ell}^{m} q_m(i).$

Krein parameters $q_{i,j}^{k}$ are the dual of the $p_{i,j}^{k}$. However they are not in general integers. Furthermore, they don't necessarily verify the "triangular inequality" relation as given in Equation (5). However there is a non-trivial (and important) subset of distance induced association schemes for which the Krein parameters verify this relation: Q-polynomial schemes.

Definition 7. *A distance induced association scheme with an ordering* $\mathbf{E}_0, \dots, \mathbf{E}_n$ *is said to be* Q*-polynomial if it satisfies the following two conditions,*

(1) $q_{i,j}^{k} = 0$ *if* $k > i + j$*, or* $|j - i| > k$ *or as soon as* $i, j, k > n$*.*
(2) $q_{1,k}^{k+1} \neq 0$ *for all* $k \in [\![0,n]\!]$*.*

This property implies in particular the 3-term order relation,

$$|\mathsf{X}| \cdot \mathbf{E}_1 \circ \mathbf{E}_j = q_{1,j}^{j-1} \mathbf{E}_{j-1} + q_{1,j}^{j} \mathbf{E}_j + q_{1,j}^{j+1} \mathbf{E}_{j+1}$$

which will be crucial in Subsection 3.4 to recover linear programming bounds from [MRRW77].

2.4. **Fourier Transforms and Convolutions.** We are now ready to introduce the Fourier transform and its inverse (usually called P and Q-transforms). All the definitions of this subsection are with respect to a fixed distance induced association scheme (X, τ, n) with an ordering $\mathbf{E}_0, \dots, \mathbf{E}_n$.

Definition 8. *Given* $f : [\![0,n]\!] \longrightarrow \mathbb{C}$*, we define its Fourier transform* $\widehat{f}$ *and its inverse Fourier transform* $\widetilde{f}$ *as follows,*

$$\widehat{f}(x) \stackrel{def}{=} \sum_{y \in [\![0,n]\!]} f(y) p_y(x) \quad , \quad \widetilde{f}(x) \stackrel{def}{=} \frac{1}{|\mathsf{X}|} \sum_{y \in [\![0,n]\!]} f(y) q_y(x).$$

Simple examples of Fourier transform and its inverse are given by,

$$\widehat{\mathbf{1}_{\{u\}}} = p_u \quad , \quad \widetilde{\mathbf{1}_{\{u\}}} = \frac{1}{|\mathsf{X}|} q_u. \tag{12}$$

When dealing with the Fourier transform and its inverse the following definition will be especially useful.

Definition 9. *Given* $f : [\![0,n]\!] \longrightarrow \mathbb{C}$*, we define its associated* $\mathbf{D}$*-matrix and* $\mathbf{E}$*-matrix as follows,*

$$\mathbf{D}^f \stackrel{def}{=} \sum_{x \in [\![0,n]\!]} f(x) \mathbf{D}_x \quad , \quad \mathbf{E}^f \stackrel{def}{=} \sum_{x \in [\![0,n]\!]} f(x) \mathbf{E}_x.$$

First notice that since $\mathbf{D}_i \circ \mathbf{D}_j = \delta_i^j \mathbf{D}_i$ and $\mathbf{E}_i \mathbf{E}_j = \delta_i^j \mathbf{E}_i$, we have,

$$\mathbf{D}^f \circ \mathbf{D}^g = \mathbf{D}^{f \cdot g} \quad , \quad \mathbf{E}^f \cdot \mathbf{E}^g = \mathbf{E}^{f \cdot g}.$$

Moreover, notice that by the decompositions given in Definitions 3 and 5, we have defined $\widehat{f}$ and $\widetilde{f}$ to ensure $\mathbf{D}^f = \mathbf{E}^{\widehat{f}}$ and $\mathbf{E}^f = \mathbf{D}^{\widetilde{f}}$ which implies by unicity in the decomposition in bases $(\mathbf{D}_i)_{i \in [\![0,n]\!]}$ and $(\mathbf{E}_i)_{i \in [\![0,n]\!]}$ that,

$$\widetilde{\widehat{f}} = \widehat{\widetilde{f}} = f. \tag{13}$$

We can now define the convolution product and reverse convolution product between functions.

Definition 10. *Given $f,g : [\![0,n]\!] \longrightarrow \mathbb{C}$, we define their convolution $\star$ and their reverse convolution $\circledast$ as follows,*

$$(f \star g)(x) \overset{def}{=} \sum_{y,z \in [\![0,n]\!]} f(y)g(z)p^x_{y,z} \quad , \quad (f \circledast g)(x) \overset{def}{=} \frac{1}{|\mathsf{X}|} \sum_{y,z \in [\![0,n]\!]} f(y)g(z)q^x_{y,z}.$$

The convolution and reverse convolution are defined to ensure $\mathbf{D}^{f\star g} = \mathbf{D}^f \cdot \mathbf{D}^g$ and $\mathbf{E}^{f \circledast g} = \mathbf{E}^f \circ \mathbf{E}^g$ which enables to prove the following proposition.

Proposition 5. *Let $f,g : [\![0,n]\!] \longrightarrow \mathbb{C}$, we have,*

$$(1)\ \widehat{f \star g} = \widehat{f} \cdot \widehat{g} \quad , \quad (2)\ \widetilde{f \circledast g} = \widetilde{f} \cdot \widetilde{g} \quad , \quad (3)\ \widehat{(fg)} = \widehat{f} \circledast \widehat{g} \quad , \quad (4)\ \widetilde{(fg)} = \widetilde{f} \star \widetilde{g}.$$

Proof. We write,

(1) $\mathbf{E}^{\widehat{f\star g}} = \mathbf{D}^{f \star g} = \mathbf{D}^f \cdot \mathbf{D}^g = \mathbf{E}^{\widehat{f}} \cdot \mathbf{E}^{\widehat{g}} = \mathbf{E}^{\widehat{f} \cdot \widehat{g}}$,
(2) $\mathbf{D}^{\widetilde{f \circledast g}} = \mathbf{E}^{f \circledast g} = \mathbf{E}^f \circ \mathbf{E}^g = \mathbf{D}^{\widetilde{f}} \circ \mathbf{D}^{\widetilde{g}} = \mathbf{D}^{\widetilde{f} \cdot \widetilde{g}}$,
(3) Use $\widehat{(f \cdot g)} = \widehat{\left(\widetilde{\widetilde{f}} \cdot \widetilde{\widetilde{g}}\right)}$ and apply (2),
(4) Use $\widetilde{(f \cdot g)} = \widetilde{\left(\widehat{\widehat{f}} \cdot \widehat{\widehat{g}}\right)}$ and apply (1),

where in (1) and (2) we conclude by using the unicity in the decomposition in bases $(\mathbf{D}_i)_{i \in [\![0,n]\!]}$ and $(\mathbf{E}_i)_{i \in [\![0,n]\!]}$. □

Finally, the fact that the Krein parameters are nonnegative implies the following.

Proposition 6. *Given $f,g : [\![0,n]\!] \longrightarrow \mathbb{R}_{\geq 0}$, we have $f \circledast g \geq 0$.*

2.5. Codes and Dual Weight Distribution.

Given a distance induced association scheme, our aim is to provide upper bounds on the size of codes with a fixed minimum distance. These objects are defined as follows.

Definition 11 (Code, distance distribution and minimum distance)**.** *Let (X, τ, n) denote a distance induced association scheme. Any subset $\mathcal{C} \subseteq \mathsf{X}$ is called a code.*

Given a code $\mathcal{C}$, we define its weight distribution as,

$$\forall t \in [\![0,n]\!], \quad a(t) \overset{def}{=} \frac{1}{|\mathcal{C}|} \cdot \left|\left\{(c,c') \in \mathcal{C}^2 : \tau(c,c') = t\right\}\right|.$$

The minimum distance of $\mathcal{C}$ is then defined as,

$$d_{\min}(\mathcal{C}) \overset{def}{=} \min\left\{\tau(c,c') : c,c' \in \mathcal{C} \text{ and } c \neq c'\right\} = \min\{t \in [\![1,n]\!] : a(t) \neq 0\}.$$

Remark 3. *We have normalized the weight distribution of codes to ensure $a(0) = 1$.*

In the remainder of this section, we will use Dirac's *bra-ket* notation for linear algebra. Dirac's notation is borrowed from quantum computing [NC10] and even though our work is unrelated with quantum computing, this notation is in our opinion an especially elegant way of presenting the results of this section, particularly the generalization of MacWilliams identities.

More concretely, let $\mathsf{X} = \{x_1, \dots, x_N\}$. From any $x_i \in \mathsf{X}$ we associate the column vector $|x_i\rangle$ whose i^{th} entry is 1 while the others are 0. Then we write $|v\rangle$ for any vector of the complex-vector space generated by the $|x_i\rangle$ for $i \in [\![1,N]\!]$. We write for example,

$$|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix} = \sum_{i=1}^{N} v_i \, |x_i\rangle \, .$$

For a column vector $|v\rangle = \begin{pmatrix} v_1 \\ \vdots \\ v_N \end{pmatrix}$, we also define the line vector,

$$\langle v| \overset{\text{def}}{=} \begin{pmatrix} \overline{v_1} & \dots & \overline{v_N} \end{pmatrix}.$$

In particular, $\langle x_i|$ is the line vector whose i^{th} entry is 1 while the others are 0. With this notation, the canonical inner product between vectors $\langle v|w\rangle$ is the multiplication $\langle v| \cdot |w\rangle$. Notice also that any rank one matrix of $\mathbb{C}(\mathsf{X}^2)$ can now be written as $|v\rangle \cdot \langle w|$ which we write $|v\rangle\langle w|$.

We now relate the weight distribution of a code $\mathcal{C}$ with the underlying $\mathbf{D}_i$ matrices of the association scheme.

Definition 12. *Given a code $\mathcal{C}$, let,*

$$|\psi_{\mathcal{C}}\rangle \overset{def}{=} \frac{1}{\sqrt{|\mathcal{C}|}} \sum_{c \in \mathcal{C}} |c\rangle .$$

This vector relates the weight distribution of a given code and underlying adjacency matrices of the association scheme. We have the following relation.

Proposition 7. *Let (X, τ, n) be a distance induced association scheme, we have,*

$$\forall t \in [\![0, n]\!], \quad a(t) = \langle \psi_{\mathcal{C}}| \mathbf{D}_t |\psi_{\mathcal{C}}\rangle . \tag{14}$$

Proof. With our notation, we have $\mathbf{D}_t = \sum_{x,x':\tau(x,x')=t} |x\rangle\langle x'|$, which gives,

$$\langle \psi_{\mathcal{C}}| \mathbf{D}_t |\psi_{\mathcal{C}}\rangle = \frac{1}{|\mathcal{C}|} \sum_{c,c' \in \mathcal{C}} \sum_{\substack{x,x' \in \mathsf{X} \\ \tau(x,x')=t}} \langle c| \cdot |x\rangle\langle x'| \cdot |c'\rangle = \frac{1}{|\mathcal{C}|} \sum_{c,c' \in \mathcal{C}} \sum_{\substack{x \in \mathsf{X} \\ \tau(x,c')=t}} \langle c|x\rangle = \frac{1}{|\mathcal{C}|} \sum_{\substack{c,c' \in \mathcal{C} \\ \tau(c,c')=t}} 1$$

which concludes the proof by definition of $a(t)$. □

The weight distribution of codes plays an important role in providing upper-bounds on their size given their minimum distance, in particular their "dual" which is defined as follows.

Definition 13 (Dual weight distribution)**.** *Let (X, τ, n) denote a distance induced association scheme with an ordering $\mathbf{E}_0, \dots, \mathbf{E}_n$. Given a code $\mathcal{C}$, we define its dual weight distribution as,*

$$a'(t) \overset{def}{=} \langle \psi_{\mathcal{C}}| \mathbf{E}_t |\psi_{\mathcal{C}}\rangle = \frac{1}{|\mathsf{X}|} \sum_{x \in [\![0,n]\!]} \langle \psi_{\mathcal{C}}| q_t(x) \mathbf{D}_x |\psi_{\mathcal{C}}\rangle = \frac{1}{|\mathsf{X}|} \sum_{x \in [\![0,n]\!]} q_t(x) a(x).$$

Interestingly, the dual weight distribution turns out to be nonnegative, result which is known as a MacWilliams identity.

Proposition 8. *Let (X, τ, n) denote a distance induced association scheme with an ordering $\mathbf{E}_0, \dots, \mathbf{E}_n$. Let $\mathcal{C} \subseteq \mathsf{X}$. Its dual weight distribution verifies,*

$$\forall t \in [\![0, n]\!], \quad a'(t) \geq 0.$$

Proof. By definition the $\mathbf{E}_t$ are projectors. Therefore we can write each $\mathbf{E}_t = \sum_i \left|v_i^t\right\rangle\!\left\langle v_i^t\right|$ for some rank 1 projectors $\left|v_i^t\right\rangle\!\left\langle v_i^t\right|$. Plugging this expression into the definition of a' leads to,

$$a'(t) = \langle \psi_{\mathcal{C}}| \mathbf{E}_t |\psi_{\mathcal{C}}\rangle = \langle \psi_{\mathcal{C}}| \sum_i \left|v_i^t\right\rangle\!\left\langle v_i^t\right| |\psi_{\mathcal{C}}\rangle = \sum_i \left|\left\langle \psi_{\mathcal{C}} \middle| v_i^t\right\rangle\right|^2 \geq 0$$

which concludes the proof. □

2.6. **Delsarte's Linear Program of Association Schemes.** Let (X,τ,n) be a distance induced association scheme. In the attempt to provide bounds on the maximum size of a code $\mathcal{C}\subseteq\mathsf{X}$ with minimum distance at least d, Delsarte introduced [Del73] the following linear program

Delsarte's Linear Program (DLP)

$$\begin{aligned} \text{maximize } \sum_{t\in[\![0,n]\!]} u(t) & \\ u(0) &= 1 \\ u(t) &= 0 \text{ for } t\in[\![1,d-1]\!] \\ u(t) &\geq 0 \text{ for } t\in[\![d,n]\!] \\ \sum_{t\in[\![0,n]\!]} u(t)q_i(t) &\geq 0 \text{ for } i\in[\![0,n]\!]. \end{aligned}$$

Definition 14. *Let (X,τ,n) be a distance induced association scheme with an ordering $\mathbf{E}_0,\dots,\mathbf{E}_n$ and $d\in[\![0,n]\!]$. We define $A_{\mathrm{LP}}(n,d)$ to be the maximum of the above linear program.*

The following proposition justifies the introduction of Delsarte's linear program to give upper bounds on the size of a code given its minimum distance.

Proposition 9. *Let $\mathcal{C}\subseteq\mathsf{X}$ be a code with minimum distance at least d. We have,*

$$|\mathcal{C}|\leq A_{\mathrm{LP}}(n,d).$$

Proof. It is a simple consequence of the fact that the weight distribution $a(t)$ of $\mathcal{C}$ verifies the condition of Delsarte's linear program, in particular the positivity of its dual weight distribution (see Definition 13) given by Proposition 8. □

The above proposition shows that solving Delsarte's linear program gives upper bounds for code sizes. Finding the value of this linear program is a hard problem. In order to find upper bounds on this linear program one has to look at the dual linear program which is a linear program such that its minimum will be larger than $A_{\mathrm{LP}}(n,d)$.

A simpler but essentially equivalent way of formulating the dual linear program is via the following proposition (see for instance [DL98, III. B]) which finds solutions to the dual linear program - and hence upper bounds $A_{\mathrm{LP}}(n,d)$ - via the choice of some function.

Proposition 10. *Let $d\in[\![0,n]\!]$ and $f:[\![0,n]\!]\longrightarrow\mathbb{R}$ be a function such that,*

$$\widehat{f}\geq 0 \quad , \quad \widehat{f}(0)>0 \quad , \quad \forall x\geq d,\ f(x)\leq 0.$$

Then,

$$A_{\mathrm{LP}}(n,d)\leq|\mathsf{X}|\cdot\frac{f(0)}{\widehat{f}(0)}.$$

Proof. Let u be a function that satisfies the constraints of the linear program and f that satisfies the requirements of the proposition. Let,

$$\forall i\in[\![0,n]\!],\quad u'(i)\overset{\text{def}}{=}\sum_{t\in[\![0,n]\!]}u(t)q_i(t)\geq 0.$$

First,

$$\sum_{x\in[\![0,n]\!]}u'(x)\widehat{f}(x)=\sum_{y\in[\![0,n]\!]}\left(\sum_{x\in[\![0,n]\!]}q_x(y)\widehat{f}(x)\right)u(y)=|\mathsf{X}|\cdot\sum_{y\in[\![0,n]\!]}\widehat{\widehat{f}}(y)u(y)=|\mathsf{X}|\cdot\sum_{y\in[\![0,n]\!]}f(y)u(y)$$

where in the last equality we used Equation (13). Therefore, we write

$$u'(0)\widehat{f}(0) \leq \sum_{x\in[\![0,n]\!]} u'(x)\widehat{f}(x) = |\mathsf{X}| \cdot \sum_{x\in[\![0,n]\!]} u(x)f(x) \leq |\mathsf{X}| \cdot u(0)f(0) = |\mathsf{X}| \cdot f(0).$$

In order to conclude, we just have to compute $u'(0) = \sum_{t\in[\![0,n]\!]} u(t)q_0(t) = \sum_{t\in[\![0,n]\!]} u(t)$ (see Equation (7)). From there,

$$\sum_{t\in[\![0,n]\!]} u(t) \leq |\mathsf{X}| \cdot \frac{f(0)}{\widehat{f}(0)}.$$

It ends the proof since this is true for any solution u of the linear program. □

Let us stress that finding functions f satisfying the above conditions corresponds to finding solutions to Delsarte's dual linear program.

3. Packing Bounds for Association Schemes

The best asymptotic upper bounds on the size of q-ary and constant-weight codes for a fixed minimum distance, *i.e.,* packing bounds, were obtained in [MRRW77] via Delsarte's Linear Program (DLP), in particular using Proposition 10. The functions that achieve the first and second linear programming bounds are rather involved and use the so-called Christoffel-Darboux formulas for orthogonal polynomials.

Here, we present three different families of functions satisfying the conditions of Proposition 10. The first function that we use is very simple as it is just a convolution of bounded indicator functions but it recovers the well-known Hamming bound which holds in any distance induced association scheme. We made the choice to present this function as our second family of functions has been deduced from this quite simple choice. It takes a similar function to which we add the coefficient $(q_1(x) - q_1(d))$. This is actually similar to the MRRW construction but here, it is f that has bounded support[(4)] while the MRRW functions have $\widehat{f}$ with bounded support. With these functions, we obtain a generalized Elias-Bassalygo bound. We are speaking here of a "generalized" Elias-Bassalygo bound as when instantiated to the Hamming association scheme we are precisely getting the bound known as Elias-Bassalygo. Our generalized Elias-Bassalygo bound is very general, it only requires a distance induced association scheme which is not the case of [MRRW77]-like bounds (see also [DL98]). Indeed, best known packing bounds obtained via DLP are also asking the association scheme to be Q-polynomial.

This situation is well illustrated by our third choice of function which recovers [MRRW77] bounds when instantiated to the Hamming and Johnson association schemes (our function slightly differs from the one in [MRRW77]). Indeed, our third and ultimate function requires the underlying association schemes to be Q-polynomial to verify conditions of Proposition 10. These functions are close to the MRRW functions but are related to the Laplacian approach and makes the link between the linear programming approach and the (dual) Laplacian approach.

3.1. Generalised Hamming Bound for the Linear Program.

In the following theorem we show that the Hamming bound, which exists in any distance induced association scheme, turns out to be an upper bound for the Delsarte's Linear Program (DLP).

Theorem 1 (Generalized Hamming Bound for DLP). *Let (X, τ, n) be a distance induced association scheme with an ordering $\mathbf{E}_0, \ldots, \mathbf{E}_n$. For any $d \in [\![1,n]\!]$, we have,*

$$A_{\mathrm{LP}}(n,d) \leq \frac{|\mathsf{X}|}{\sum_{x=0}^{\lfloor \frac{d-1}{2} \rfloor} v_x}.$$

[(4)] In the sense that the support is restricted in $[\![0,r]\!]$ with r significantly smaller than n

Proof. Our proof strategy will be to construct a good function f which satisfies the requirements of Proposition 10. We choose,

$$f \overset{\text{def}}{=} \mathbf{1}_{\le\lfloor\frac{d-1}{2}\rfloor} \star \mathbf{1}_{\le\lfloor\frac{d-1}{2}\rfloor} \quad \text{where } \mathbf{1}_{\le\lfloor\frac{d-1}{2}\rfloor} \overset{\text{def}}{=} \sum_{x=0}^{\lfloor\frac{d-1}{2}\rfloor} \mathbf{1}_{\{x\}}.$$

We have,

$$f(x) = \sum_{y,z\in[\![0,n]\!]} \mathbf{1}_{\le\lfloor\frac{d-1}{2}\rfloor}(y)\mathbf{1}_{\le\lfloor\frac{d-1}{2}\rfloor}(z)p_{y,z}^{x} = \sum_{y,z=0}^{\lfloor\frac{d-1}{2}\rfloor} p_{y,z}^{x}.$$

Let $h = \mathbf{1}_{\le\lfloor\frac{d-1}{2}\rfloor}$. Since $f = h \star h$, we have $\widehat{f} = (\widehat{h})^2$ which gives

$$\widehat{f}(x) = \left(\sum_{y\in[\![0,n]\!]} \mathbf{1}_{\le\lfloor\frac{d-1}{2}\rfloor}(y)p_y(x)\right)^2 = \left(\sum_{y=0}^{\lfloor\frac{d-1}{2}\rfloor} p_y(x)\right)^2.$$

We clearly have $\widehat{f} \ge 0$ and $\widehat{f}(0) > 0$. Also, using Equation (5), we have $f(x) = 0$ when $x \ge d \ge 2\left\lfloor\frac{d-1}{2}\right\rfloor$. This means the conditions of Proposition 10 are satisfied. We now compute by Equations (6) and (8),

$$f(0) = \sum_{y,z=0}^{\lfloor\frac{d-1}{2}\rfloor} p_{y,z}^{0} = \sum_{y=0}^{\lfloor\frac{d-1}{2}\rfloor} v_y,$$

$$\widehat{f}(0) = \left(\sum_{y=0}^{\lfloor\frac{d-1}{2}\rfloor} p_y(0)\right)^2 = \left(\sum_{y=0}^{\lfloor\frac{d-1}{2}\rfloor} v_y\right)^2.$$

We can now use Proposition 10,

$$A_{\mathrm{LP}}(n,d) \le |\mathsf{X}| \cdot \frac{f(0)}{\widehat{f}(0)} = \frac{|\mathsf{X}|}{\sum_{y=0}^{\lfloor\frac{d-1}{2}\rfloor} v_y}$$

which concludes the proof. □

3.2. **Generalized Elias-Bassalygo Bound for the Linear Program.** Here, we start again from a function $f = \mathbf{1}_u \star \mathbf{1}_u \ge 0$ and we do the following changes: we will take u which is a little bit larger than $\lfloor\frac{d-1}{2}\rfloor$. This seems problematic since the function will be nonnegative for values above d. To circumvent this, we also multiply by the function by the term $(q_1(x) - q_1(d))$. This will ensure that the function f has the good sign conditions and we show that it is possible to choose u above $\lfloor\frac{d-1}{2}\rfloor$ while at the same time preserbing the positivity of $\widehat{f}$.

Theorem 2 (Generalized Elias-Bassalygo Bound for DLP)**.** *Let* (X, τ, n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0, \ldots, \mathbf{E}_n$ *and* $d \in [\![1,n]\!]$. *Suppose that* q_1 *is decreasing. Let,*

$$u \in \left\{u_0 \in [\![0,n]\!] : \frac{q_1(u_0)^2}{q_1(0)} \ge q_1(d) + 1\right\} \tag{15}$$

Then,

$$A_{\mathrm{LP}}(n,d) \le (q_1(0) - q_1(d)) \cdot \frac{|\mathsf{X}|}{v_u}.$$

Proof. Again, our strategy is to find a good function to use in Proposition 10. The function f that we use is,

$$f(x) \overset{\text{def}}{=} (q_1(x) - q_1(d)) \cdot (\mathbf{1}_{\{u\}} \star \mathbf{1}_{\{u\}})(x).$$

As q_1 is decreasing and $\mathbf{1}_{\{u\}} \star \mathbf{1}_{\{u\}} \ge 0$, we have that $f(x) \le 0$ for $x \ge d$.

Let us compute $\widehat{f}$. Let $h = \mathbf{1}_u \star \mathbf{1}_u$. We compute by using Proposition 5,

$$\widehat{h} = \left(\widehat{\mathbf{1}_{\{u\}}}\right)^2 = p_u^2 \quad , \quad \widehat{q_1} = |\mathsf{X}| \cdot \mathbf{1}_{\{1\}}.$$

We have $f = q_1 h - q_1(d)h$ so using again Proposition 5, we obtain,

$$\widehat{f} = \widehat{q_1} \circledast \widehat{h} - q_1(d)\widehat{h},$$

from which we deduce,

$$\widehat{f} = |\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast p_u^2 - q_1(d) \cdot p_u^2. \tag{16}$$

Let us admit for now that,

$$\widehat{f} \geq p_u^2 \geq 0 \tag{17}$$

which enables to apply Proposition 10.

We can now compute (with Equations (6) and (8)),

$$\begin{aligned} f(0) &= (q_1(0) - q_1(d)) \cdot (\mathbf{1}_{\{u\}} \star \mathbf{1}_{\{u\}})(0) = (q_1(0) - q_1(d)) \cdot p_{u,u}^0 = (q_1(0) - q_1(d)) \cdot v_u, \\ \widehat{f}(0) &\geq p_u(0)^2 = v_u^2 > 0. \end{aligned}$$

Plugging this into Proposition 10, we obtain,

$$A_{\mathrm{LP}}(n,d) \leq |\mathsf{X}| \cdot \frac{f(0)}{\widehat{f}(0)} \leq (q_1(0) - q_1(d)) \cdot \frac{|\mathsf{X}|}{v_u}.$$

To conclude it remains to prove Equation (17). To this aim, according to Equation (16), let us give a lower bound on $\mathbf{1}_{\{1\}} \circledast p_u^2$. We have the following computation,

$$\begin{aligned} \mathbf{1}_{\{1\}} \circledast p_u^2(x) &= \frac{1}{|\mathsf{X}|} \sum_{y \in [\![0,n]\!]} p_u^2(y) q_{y,1}^x \\ &\geq \frac{1}{|\mathsf{X}|} \frac{1}{\sum_{y \in [\![0,n]\!]} q_{y,1}^x} \left(\sum_{y \in [\![0,n]\!]} p_u(y) q_{y,1}^x \right)^2 \qquad \left(\text{By convexity of } x \mapsto x^2\right) \\ &= \frac{|\mathsf{X}|}{q_1(0)} \left(\mathbf{1}_{\{1\}} \circledast p_u(x)\right)^2 \end{aligned} \tag{18}$$

where in the last equality we used Equation (10). Now we write,

$$\mathbf{E}^{\mathbf{1}_{\{1\}} \circledast p_u} = \mathbf{E}_1 \circ \mathbf{E}^{p_u} = \mathbf{E}_1 \circ \mathbf{D}_u = \frac{1}{|\mathsf{X}|} \left(\sum_{j \in [\![0,n]\!]} q_1(j) \mathbf{D}_j \right) \circ \mathbf{D}_u = \frac{q_1(u)}{|\mathsf{X}|} \mathbf{D}_u = \frac{q_1(u)}{|\mathsf{X}|} \mathbf{E}^{p_u}$$

from which we obtain $\mathbf{1}_{\{1\}} \circledast p_u = \frac{q_1(u)}{|\mathsf{X}|} p_u$. Plugging this into Equation (18) leads to,

$$\mathbf{1}_{\{1\}} \circledast p_u^2(x) \geq \frac{q_1(u)^2}{q_1(0)\,|\mathsf{X}|}\, p_u^2(x) \geq \frac{(q_1(d)+1)}{|\mathsf{X}|} p_u^2(x)$$

where in the inequality we used the assumption on u. Therefore, plugging this into Equation (16) gives,

$$\widehat{f} \geq (q_1(d)+1)p_u^2 - q_1(d)p_u^2 = p_u^2$$

which concludes the proof. □

Remark 4. *When instantiating the above theorem, we will choose u satisfying Condition (15) but which maximizes v_u in order to to get the best upper bound as possible.*

3.3. **The Dual Laplacian Argument.** Here, we give general statements showing how to use a function f satisfying,

$$\mathbf{1}_{\{1\}} \circledast \widehat{f} \geq \lambda \widehat{f}$$

and certain properties to find functions satisfying the requirements of Proposition 10. The proof of the generalized Elias-Bassalygo bound is implicitly using this approach via the following claim.

Proposition 11. *Let* (X, τ, n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0, \ldots, \mathbf{E}_n$*. Let* $d \in [\![0, n]\!]$ *and let* $f : [\![0, n]\!] \longrightarrow \mathbb{R}$ *such that,*

$$|\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{f} \geq (q_1(d) + 1)\widehat{f} \quad , \quad \widehat{f} \geq 0 \quad , \quad \widehat{f}(0) > 0 \quad , \quad f \geq 0 \tag{19}$$

with q_1 *decreasing. Then we have,*

$$A_{\mathrm{LP}}(n, d) \leq (q_1(0) - q_1(d)) \cdot |\mathsf{X}| \cdot \frac{f(0)}{\widehat{f}(0)}.$$

Proof. We take $g(x) \overset{\text{def}}{=} (q_1(x) - q_1(d)) \cdot f$. We have $g(x) \leq 0$ for $x \geq d$ since q_1 is decreasing and $f \geq 0$. Furthermore, by assumption on $\widehat{f}$,

$$\widehat{g} = |\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{f} - q_1(d)\widehat{f} \geq \widehat{f} \geq 0.$$

This means g satisfies the constraints of Proposition 10. We also have, $g(0) = (q_1(0) - q_1(d)) \cdot f(0)$ and $\widehat{g}(0) \geq \widehat{f}(0) > 0$. Therefore we obtain,

$$A_{\mathrm{LP}}(n, d) \leq |\mathsf{X}| \cdot \frac{g(0)}{\widehat{g}(0)} \leq (q_1(0) - q_1(d)) \cdot |\mathsf{X}| \cdot \frac{f(0)}{\widehat{f}(0)}$$

which concludes the proof. □

Notice that in the previous proposition we asked the function f to be nonnegative which is quite restrictive. Fortunately, we can apply the above strategy (in the choice of f) by enforcing its square to appear in order to ensure the positivity. However, it is at the cost of an extra convolution on the Fourier transform but it preserves the "eigenvalue property", *i.e.,* $\mathbf{1}_{\{1\}} \circledast \widehat{f} \geq \lambda \cdot \widehat{f}$, and more importantly, it enables more functions.

Proposition 12. *Let* (X, τ, n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0, \ldots, \mathbf{E}_n$ *with* q_1 *decreasing. Let* $d \in [\![0, n]\!]$ *and let* $f : [\![0, n]\!] \longrightarrow \mathbb{R}$ *such that,*

$$|\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{f} \geq (q_1(d) + 1)\widehat{f} \quad , \quad \widehat{f} \geq 0 \quad , \quad \widehat{f}(0) > 0 \tag{20}$$

Then we have,

$$A_{\mathrm{LP}}(n, d) \leq (q_1(0) - q_1(d)) \cdot |\mathsf{X}| \cdot \frac{f^2(0)}{(\widehat{f} \circledast \widehat{f})(0)}.$$

Proof. The key point is to observe that,

$$|\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{f} \circledast \widehat{f} \geq (q_1(d) + 1)(\widehat{f} \circledast \widehat{f}).$$

Indeed, let $h \overset{\text{def}}{=} |\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{f} - (q_1(d) + 1)\widehat{f}$. Notice that by assumption $h \geq 0$. Therefore,

$$|\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{f} \circledast \widehat{f} - (q_1(d) + 1)(\widehat{f} \circledast \widehat{f}) = h \circledast \widehat{f} \geq 0$$

by Proposition 6 since both h and $\widehat{f}$ are nonnegative. Recall now that by Proposition 5,

$$\widehat{f} \circledast \widehat{f} = \widehat{(f^2)}.$$

Also, $\widehat{(f^2)}(0) = (\widehat{f} \circledast \widehat{f})(0) \geq \widehat{f}(0)^2 > 0$. This means that we have,

$$|\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{(f^2)} \geq (q_1(d) + 1)\widehat{(f^2)} \quad , \quad \widehat{(f^2)} = \widehat{f} \circledast \widehat{f} \geq 0 \quad , \quad \widehat{(f^2)}(0) > 0 \quad , \quad f^2 \geq 0.$$

We can therefore use the previous proposition with f^2. We obtain,

$$A_{\mathrm{LP}}(n,d) \le (q_1(0) - q_1(d)) \cdot |\mathsf{X}| \cdot \frac{f^2(0)}{(\widehat{f} \circledast \widehat{f})(0)}$$

which concludes the proof. □

3.4. **MRRW Bounds Using the Laplacian Method.** The last proposition of the above subsection can be used to derive packing bounds which turn out to be known as *MRRW bounds*. Indeed, when instantiated to the Hamming and Johnson association schemes we exactly recover bounds from [MRRW77].

Theorem 3 (MRRW Bound for DLP). *Let (X, τ, n) be a distance induced association scheme with an ordering $\mathbf{E}_0, \dots, \mathbf{E}_n$ which is also Q-polynomial and let $d \in [\![0,n]\!]$. Furthermore, suppose that q_1 is decreasing. Let $r^\perp$ be an integer in $[\![0,n]\!]$ such that,*

$$q_1(d) + 1 \le q_1(r^\perp).$$

We suppose that there exists $x \in [\![1,n]\!]$ such that $q_x(r^\perp) \le 0$ and we define,

$$r \overset{def}{=} \min\left\{x \in [\![1,n]\!] : \; q_x(r^\perp) \le 0\right\} = \min\left\{x \in [\![1,n]\!] : \; p_{r^\perp}(x) \le 0\right\}.$$

Then,

$$A_{\mathrm{LP}}(n,d) \le (q_1(0) - q_1(d)) \cdot \sum_{x \in [\![0,r-1]\!]} m_x.$$

To prove this theorem we will rely on the following function.

Proposition 13. *Let (X, τ, n) be a distance induced association scheme with an ordering $\mathbf{E}_0, \dots, \mathbf{E}_n$ which is also Q-polynomial. Let f be the function such that,*

$$\forall x \in [\![0,n]\!], \quad \widehat{f}(x) \overset{def}{=} \begin{cases} \frac{q_x(r^\perp)}{m_x} & \text{if } x \in [\![0,r-1]\!] \\ 0 & \text{otherwise} \end{cases}$$

where r and $r^\perp$ are defined as in Theorem 3. Then,

$$(i)\ \widehat{f} \ge 0, \quad (ii)\ \widehat{f}(0) > 0, \quad \text{and} \quad (iii)\ |\mathsf{X}| \cdot \mathbf{1}_{\{1\}} \circledast \widehat{f} \ge q_1(r^\perp) \cdot \widehat{f}.$$

Proof. By assumption on r we have for all $x \in [\![0,r-1]\!]$, $q_x(r^\perp) \ge 0$ showing that $\widehat{f}$ is nonnegative. Furthermore, $\widehat{f}(0) = q_0(r^\perp)/m_0 = 1$. Let us now show that condition (iii) holds. First,

$$\begin{aligned}
\forall x \in [\![0,r-2]\!], \quad (\mathbf{1}_{\{1\}} \circledast \widehat{f})(x) &= \frac{1}{|\mathsf{X}|} \sum_{y \in [\![0,r-1]\!]} \widehat{f}(y) q_{1,y}^x \\
&= \frac{1}{|\mathsf{X}|} \sum_{y \in [\![0,r-1]\!]} \frac{q_{1,y}^x}{m_y} q_y(r^\perp) \\
&= \frac{1}{|\mathsf{X}|} \sum_{y \in [\![0,r-1]\!]} \frac{q_{1,x}^y}{m_x} q_y(r^\perp) \quad \text{(By Equation (11))} \\
&= \frac{1}{|\mathsf{X}|} \frac{1}{m_x} q_1(r^\perp) q_x(r^\perp) \\
&= \frac{q_1(r^\perp) \widehat{f}(x)}{|\mathsf{X}|}
\end{aligned}$$

where we used Proposition 4 combined with the fact that the scheme is supposed to be Q-polynomial (see Definition 7) and the $q_{i,j}^k$ are equal to 0 if one i, j, k is greater than the sum of the other two. Furthermore, using once again this assumption,

$$\begin{aligned}
(\mathbf{1}_{\{1\}} \circledast \widehat{f})(r-1) &= \frac{1}{|\mathsf{X}|}\left(q^{r-1}_{1,r-2}\widehat{f}(r-2) + q^{r-1}_{1,r-1}\widehat{f}(r-1) + q^{r-1}_{1,r}\widehat{f}(r)\right) \\
&= \frac{1}{|\mathsf{X}|}\left(\frac{q^{r-1}_{1,r-2}}{m_{r-2}} q_{r-2}(r^{\perp}) + \frac{q^{r-1}_{1,r-1}}{m_{r-1}} q_{r-1}(r^{\perp})\right) \\
&= \frac{1}{|\mathsf{X}|}\left(\frac{q^{r-2}_{1,r-1}}{m_{r-1}} q_{r-2}(r^{\perp}) + \frac{q^{r-1}_{1,r-1}}{m_{r-1}} q_{r-1}(r^{\perp})\right) \quad \text{(By Equation (11))} \\
&\geq \frac{1}{|\mathsf{X}|\, m_{r-1}}\left(q^{r-2}_{1,r-1} q_{r-2}(r^{\perp}) + q^{r-1}_{1,r-1} q_{r-1}(r^{\perp}) + q^{r-1}_{1,r} q_{r}(r^{\perp})\right) \\
&= \frac{1}{|\mathsf{X}|\, m_{r-1}} q_1(r^{\perp}) q_{r-1}(r^{\perp}) = \frac{q_1(r^{\perp})\widehat{f}(r-1)}{|\mathsf{X}|}
\end{aligned}$$

where we used for the inequality $q^{r-1}_{1,r} q_r(r^{\perp}) \leq 0$ coming from the definition of r and the positivity of the $q^{k}_{i,j}$ (see Proposition 3). Finally,

$$(\mathbf{1}_{\{1\}} \circledast \widehat{f})(r) = \sum_{y \in [\![0,r+1]\!]} \widehat{f}(y) q^{r}_{1,y} = \widehat{f}(r-1) q^{r}_{1,r-1} \geq 0$$

and $\forall x > r,\ (\mathbf{1}_{\{1\}} \circledast \widehat{f})(x) = 0$. From there, we deduce that,

$$\forall x \in [\![r,n]\!], \quad (\mathbf{1}_{\{1\}} \circledast \widehat{f})(x) \geq 0 = \frac{q_1(r^{\perp})}{|\mathsf{X}|}\widehat{f}(x)$$

which concludes the proof. □

Proof of Theorem 3. First, the equality when defining $r^{\perp}$ comes from Proposition 2. Let us now take f as defined in the above proposition. Recall that by assumption,

$$q_1(d) + 1 \leq q_1(r^{\perp}).$$

We can therefore apply Proposition 12 (here is used the assumption that q_1 is a decreasing function) with the above function f. We get,

$$\widehat{f} \circledast \widehat{f}(0) = \frac{1}{|\mathsf{X}|} \sum_{x \in [\![0,n]\!]} \widehat{f}(x)^2 q^{0}_{x,x} = \frac{1}{|\mathsf{X}|} \sum_{x \in [\![0,r-1]\!]} \widehat{f}(x)^2 m_x$$

where in the last equality we used Equation (9). Furthermore,

$$\begin{aligned}
f^2(0) = \widetilde{\widehat{f}}(0)^2 &= \frac{1}{|\mathsf{X}|^2}\left(\sum_{y \in [\![0,n]\!]} \widehat{f}(y) q_y(0)\right)^2 \\
&= \frac{1}{|\mathsf{X}|^2}\left(\sum_{y \in [\![0,r-1]\!]} \widehat{f}(y) m_y\right)^2 \quad \text{(By Equation (8))} \\
&\leq \frac{1}{|\mathsf{X}|^2}\left(\sum_{y \in [\![0,r-1]\!]} m_y\right)\left(\sum_{y \in [\![0,r-1]\!]} \widehat{f}(y)^2 m_y\right)
\end{aligned}$$

where in the last inequality we used the Cauchy-Schwartz inequality. From there, we get by applying Proposition 12,

$$A_{\mathrm{LP}}(n,d) \leq (q_1(0) - q_1(d))|\mathsf{X}|\frac{f^2(0)}{(\widehat{f} \circledast \widehat{f})(0)} \leq (q_1(0) - q_1(d)) \cdot \sum_{y \in [\![0,r-1]\!]} m_y$$

which concludes the proof. □

4. Applications: Packing Bounds for q-ary and Constant-Weight Binary Codes

We are interested in this section to give upper bounds on the size of q-ary and constant-weight binary codes, *i.e.,* subsets of $\mathbb{F}_q^n$ and $\mathcal{S}_a^{n,2}$ (words of Hamming weight a in $\mathbb{F}_2^n$), for a fixed minimum distance. Bounds will also be presented asymptotically in n and in order to describe them compactly let us introduce some notation. We define $A^{(q)}(n,d)$ (*resp.* $A(n,d,a)$) to be the largest possible codes of $\mathbb{F}_q^n$ (*resp.* $\mathcal{S}_a^{n,2}$) with minimum *Hamming distance* at least d. Next we define,

$$R^{(q)}(\delta) \overset{\text{def}}{=} \overline{\lim_{n\to+\infty}} \frac{1}{n}\log_q A(n,\lfloor \delta n\rfloor) \quad \left(\text{resp. } R(\delta,\alpha) \overset{\text{def}}{=} \overline{\lim_{n\to+\infty}} \frac{1}{n}\log_2 A(n,\lfloor \delta n\rfloor,\lfloor \alpha n\rfloor)\right)$$

Upper bounds over $R^{(q)}(\delta)$ will involve the q-ary entropy,

$$h_q : x \in [0,1] \longmapsto -(1-x)\log_q(1-x) - x\log_q\left(\frac{x}{q-1}\right).$$

This function gives the asymptotic behaviour of the binomial coefficients as shown in the following elementary lemma which will be at the core of all asymptotic results of this section.

Lemma 1. *Let $t \overset{def}{=} \lfloor \tau n\rfloor$, we have,*

$$\frac{1}{n}\log_q \binom{n}{t}(q-1)^t \underset{n\to+\infty}{=} h_q(\tau) + o(1).$$

4.1. **Hypercube Case.** We instantiate in this subsection packing-bounds from the previous section in the Hamming scheme $(\mathbb{F}_q^n, \tau_{\mathrm{H}}, n)$ where τ_{H} denotes the Hamming distance. This association scheme comes with a canonical ordering $\mathbf{E}_0,\dots,\mathbf{E}_n$. We give in what follows all the fundamental parameters of this association scheme with respect to this ordering as well as required properties to apply Theorems 1, 2 and 3. We refer the reader to [DL98].

First, $(\mathbb{F}_q^n, \tau_{\mathrm{H}}, n)$ is a distance induced association scheme which is also Q-polynomial.

Its valencies and multiplicities are given by,

$$\forall i \in [\![0,n]\!], \quad v_i = m_i = \binom{n}{i}(q-1)^i. \tag{21}$$

The p and q-numbers of the Hamming scheme involve *Krawtchouk polynomials* $K_k^{n,q}$ which are defined as follows,

$$\forall k \in [\![0,n]\!], \quad K_k^{n,q}(X) \overset{\text{def}}{=} \sum_{j\in[\![0,k]\!]} (-1)^j (q-1)^{k-j}\binom{X}{j}\binom{n-X}{k-j}$$

where $\binom{X}{i} \overset{\text{def}}{=} X(X-1)\cdots(X-i+1)/i!$. More precisely, p and q-numbers are the integers given by the evaluation of the Krawtchouk polynomials over $[\![0,n]\!]$, *i.e.,*

$$\forall i,k \in [\![0,n]\!], \quad q_k(i) = p_k(i) = K_k^{n,q}(i).$$

Then it is readily seen that,

$$\forall i \in [\![0,n]\!], \quad q_1(i) = (q-1)(n-i) - i = (q-1)n - qi$$

which is a decreasing function as required in Theorems 2 and 3. We denote $A_{\mathrm{LP}}^{(q)}(n,d)$ the maximum value of the associated linear program (as per Subsection 2.6) and we define,

$$R_{\mathrm{LP}}^{(q)}(\delta) \overset{\text{def}}{=} \overline{\lim_{n\to+\infty}} \frac{1}{n}\log_q A_{\mathrm{LP}}^{(q)}(n,\lfloor \delta n\rfloor).$$

We immediately deduce from Proposition 9 that,

$$A^{(q)}(n,d) \le A_{\mathrm{LP}}^{(q)}(n,d) \quad , \quad R^{(q)}(\delta) \le R_{\mathrm{LP}}^{(q)}(\delta).$$

Hamming Bound. By using the valencies of $(\mathbb{F}_q^n, \tau_{\mathrm{H}}, n)$ and Theorem 1 we easily recover the Hamming bound.

Theorem 4 (Hamming Bound for $A_{\mathrm{LP}}^{(q)}(n,d)$)**.** *For any $q,n \geq 2$ and $d \geq 1$,*

$$A^{(q)}(n,d) \leq A_{\mathrm{LP}}^{(q)}(n,d) \leq \frac{q^n}{\sum_{x=0}^{\lfloor \frac{d-1}{2} \rfloor} v_x} = \frac{q^n}{\sum_{x=0}^{\lfloor \frac{d-1}{2} \rfloor} (q-1)^x \binom{n}{x}},$$

which implies asymptotically,

$$R^{(q)}(\delta) \leq R_{\mathrm{LP}}^{(q)}(\delta) \leq 1 - h_q(\delta/2).$$

Elias-Bassalygo Bound. Let us now instantiate to the hypercube our generalized Elias-Bassalygo bound of Theorem 2. As we show we indeed recover the bound classically known as Elias-Bassalygo.

Theorem 5 (Elias-Bassalygo Bound for $A_{\mathrm{LP}}^{(q)}(n,d)$)**.** *For any $q,n \geq 2$ and $d \in [\![0, \lfloor n(q-1)/q \rfloor]\!]$, we have,*

$$A^{(q)}(n,d) \leq A_{\mathrm{LP}}^{(q)}(n,d) \leq qd \cdot \frac{q^n}{\binom{n}{u}(q-1)^u}, \quad \textit{where} \quad u \overset{def}{=} \left\lfloor n \frac{q-1}{q} \cdot \left(1 - \sqrt{1 - \frac{qd-1}{(q-1)n}}\right)\right\rfloor.$$

It implies asymptotically for any $\delta \in [0, (q-1)/q]$,

$$R^{(q)}(\delta) \leq R_{\mathrm{LP}}^{(q)}(\delta) \leq 1 - h_q(J_q(\delta)), \quad \textit{where} \quad J_q(\delta) \overset{def}{=} \frac{q-1}{q} \cdot \left(1 - \sqrt{1 - \frac{q\delta}{(q-1)}}\right).$$

Proof. Our strategy is to apply Theorem 2. First q_1 is indeed a decreasing function. Now, let us compute,

$$u \in \left\{u_0 \in [\![0,n]\!] : \frac{q_1(u_0)^2}{q_1(0)} \geq q_1(d) + 1\right\} \text{ which maximizes } \binom{n}{u}(q-1)^u.$$

We have the following computation,

$$q_1(0)\left(q_1(d)+1\right) = (q-1)n\left((q-1)n - qd + 1\right) = ((q-1)n)^2 \left(1 - \frac{qd-1}{(q-1)n}\right)$$

Since $d \leq n(q-1)/q$, the right hand side term is non negative and we therefore have

$$q_1(u_0)^2 \geq q_1(0)\left(q_1(d)+1\right) \Leftrightarrow (q-1)n - qu_0 \geq (q-1)n\sqrt{1 - \frac{qd-1}{(q-1)n}}$$

showing that we have to choose u smaller than,

$$\left\lfloor n \frac{q-1}{q} \cdot \left(1 - \sqrt{1 - \frac{qd-1}{(q-1)n}}\right)\right\rfloor.$$

We can choose u as above as $y \mapsto \binom{n}{y}(q-1)^y$ is an increasing function over $\left[\!\left[0, \left\lfloor n\,\frac{q-1}{q}\right\rfloor\right]\!\right]$. Applying Theorem 2, we obtain,

$$A_{\mathrm{LP}}^{(q)}(n,d) \leq (q_1(0) - q_1(d))\frac{q^n}{v_u} = qd \cdot \frac{q^n}{\binom{n}{u}(q-1)^u}.$$

The asymptotic result easily follows from Lemma 1. □

MRRW1 Bound. We now instantiate the bound from Theorem 3 to the Hamming scheme. We recover the bound from [MRRW77, Eq. (2.6)] but in the q-ary setting ([MRRW77] restricts to the case $q = 2$ but it was generalized for example in [DL98]).

Theorem 6 (MRRW1-type Bound for $A_{\mathrm{LP}}^{(q)}(n,d)$)**.** *Let integers $q,n \geq 2$ and $d \in [\![1, \lfloor n(q-1)/q \rfloor]\!]$. Let $r = \lceil \zeta_{d-1} \rceil$, where ζ_{d-1} is the first zero of $K_{d-1}^{n,q}(X)$. Then,*

$$A^{(q)}(n,d) \leq A_{\mathrm{LP}}^{(q)}(n,d) \leq qd \cdot \sum_{x=0}^{r-1} (q-1)^x \binom{n}{x},$$

which implies asymptotically for any $\delta \in [0,(q-1)/q]$,

$$R^{(q)}(\delta) \le R^{(q)}_{\mathrm{LP}}(\delta) \le h_q\left(\gamma_q(\delta)\right) \;\; \textit{where} \;\; \gamma_q(\delta) \overset{def}{=} \frac{1}{q}\left(q-1-(q-2)\delta - 2\sqrt{(q-1)\delta(1-\delta)}\right).$$

Proof. Our goal is to apply Theorem 3. First, notice that $q_1(d)+1 \le q_1(d-1)$ so we choose $r^\perp = d-1$. Let $r = \lceil \zeta_{r^\perp} \rceil$ where $\zeta_{r^\perp}$ denotes the first zero of $K^{n,q}_{r^\perp}(X)$ in $[0,n]$. We know that the zeros of this polynomial are all in this interval and are simple. Furthermore, there is always an integer between any two consecutive zeros [CS90]. Therefore, as $K^{n,q}_{r^\perp}(0) = v_{r^\perp} > 0$, we obtain by continuity,

$$\begin{aligned} q_r(r^\perp) &= \frac{m_r}{v_{r^\perp}}\, p_{r^\perp}(r) = \frac{m_r}{v_{r^\perp}}\, K^{n,q}_{r^\perp}(r) \le 0, \\ \forall x \in [\![0,r-1]\!],\;\; q_x(r^\perp) &= \frac{m_x}{v_{r^\perp}}\, p_{r^\perp}(x) = \frac{m_x}{v_{r^\perp}}\, K^{n,q}_{r^\perp}(x) > 0. \end{aligned}$$

This shows that $r^\perp$ and r satisfy the conditions of Theorem 3, which gives,

$$A^{(q)}_{\mathrm{LP}}(n,d) \le (q_1(0)-q_1(d)) \cdot \sum_{x=0}^{r-1} m_r = qd \cdot \sum_{x=0}^{r-1} (q-1)^x \binom{n}{x}.$$

We now prove the asymptotic part of the proposition for a fixed $\delta \in (0,(q-1)/q)$. The asymptotic part of the proposition follows from the asymptotic expansion of ζ_x (which denotes the first root of $K^{n,q}_x(X)$). Indeed, given $x \in [\![0,n]\!]$ such that $x/n \underset{n\to+\infty}{\longrightarrow} \alpha \in [0,(q-1)/q]$, we have [DL98, §IV. F],

$$\frac{\zeta_x}{n} \underset{n\to+\infty}{=} \gamma_q(\alpha) + o(1).$$

In our case, $r^\perp/n = (d-1)/n \underset{n\to+\infty}{\longrightarrow} \delta \in [0,(q-1)/q]$ (where $d = \lfloor \delta n \rfloor$). Therefore $r/n = \lceil \zeta_{r^\perp} \rceil / n \underset{n\to+\infty}{\longrightarrow} \gamma_q(\delta)$. We can conclude using Lemma 1 that $R^{(q)}_{\mathrm{LP}}(\delta) \le h_q(\gamma_q(\delta))$. □

Discussion. We now recap in Figure 3 the asymptotic upper bounds over $R^{(q)}(\delta)$ obtained in Theorems 4, 5 and 6 in the binary case, *i.e.*, $q=2$. We have also added the best known upper bound on $R(\delta)$: the second linear programming bound from [MRRW77, Eq. (1.4)]. As we mentioned in the introduction, the latter was obtained in [MRRW77] via an upper bound over constant-weight binary codes and not directly via the linear program derived from the Hamming scheme. More precisely, [MRRW77] used first the following bound (which turns out to be the key inequality to obtain the Elias-Bassalygo bound via combinatorial arguments),

$$\forall a \in [\![0,\lfloor n/2 \rfloor]\!], \quad A^{(2)}(n,d) \le \frac{2^n}{\binom{n}{a}}\, A(n,d,a).$$

Therefore, providing upper bounds on $A^{(2)}(n,d)$ can be reduced to finding upper bounds on $A(n,d,a)$ and then optimizing over the radius a. To obtain good bounds on $A(n,d,a)$, [MRRW77] relied on the linear program derived from the Johnson sphere. We will proceed similarly in the next subsection by instantiating Theorems 1, 2 and 3 in this context.

Though the second linear programming bound was obtained thanks to a solution of the linear program derived from the Johnson scheme, Rodemich [Rod80] showed how to turn the latter into a solution of the linear program derived this time from the Hamming scheme. In other words, Rodemich's result shows that there exists a better solution of the linear program in the Hamming scheme than the one obtained in [MRRW77] and ours. However this result only holds in the binary setting. Indeed, in the q-ary setting the Johnson scheme does not yield an association scheme, and therefore Delsarte's approach does not apply, *i.e.*, there are no linear program to solve. But it can be proved that the Elias-Bassalygo bound is better for any q than the bound derived from

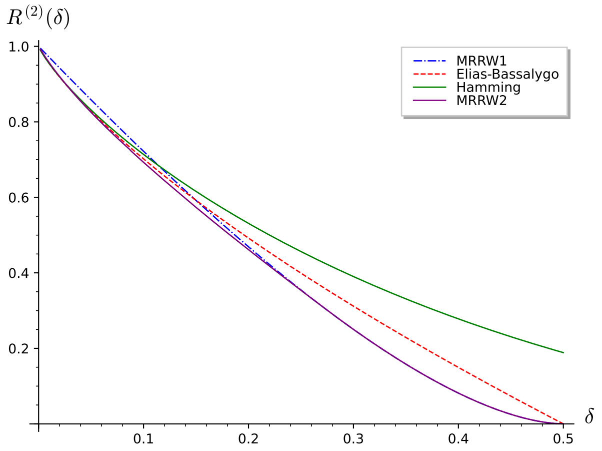

FIGURE 3. Upper bounds over $R^{(2)}(\delta)$ via the linear program with the Hamming (Theorem 4), Elias-Bassalygo (Theorem 5), MRWW1 (Theorem 6) bounds and MRRW2 being the second linear programming bound [MRRW77, Eq. (1.4)].

Theorem 6 (which corresponds to the first linear programming bound of [MRRW77] instantiated in the q-ary case). In other words, as Rodemich's idea does not apply when $q > 2$, our work has exhibited for this setting and small minimum distances, a solution which is better than all previously known solutions of the linear program derived from the Hamming scheme. By way of illustration we give in Figure 4 the asymptotic upper bounds over $R^{(q)}(\delta)$ obtained in Theorems 4, 5 and 6 for some $q > 2$.

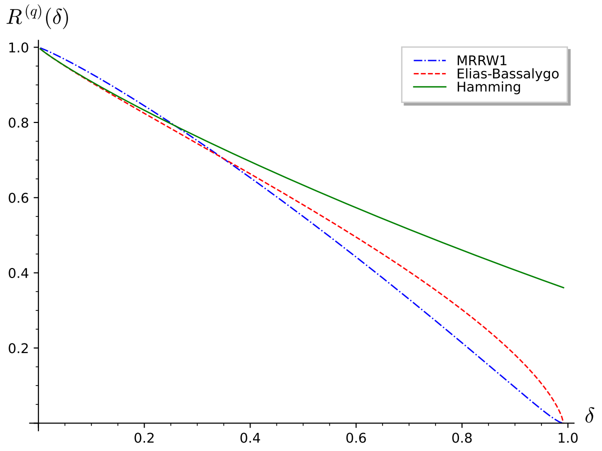

FIGURE 4. Upper bounds over $R^{(q)}(\delta)$ via the linear program with the Hamming (Theorem 4), Elias-Bassalygo (Theorem 5) and MRWW1 (Theorem 6) for $q = 121$.

4.2. **Johnson Sphere and Relation to the Hamming Cube.** We consider now the Johnson scheme $(\mathcal{S}_a^{n,2}, \tau_{\mathrm{J}} = \tau_{\mathrm{H}}/2, a)$ where $\mathcal{S}_a^{n,2}$ denotes the set of words of Hamming weight $a \in [\![0, \lfloor n/2 \rfloor]\!]$ in the Hamming cube $\mathbb{F}_2^n$. It is a distance induced scheme with a canonical ordering $\mathbf{E}_0, \dots, \mathbf{E}_a$ which is also Q-polynomial [DL98]. Its valencies and multiplicities are given by,

$$\forall i \in [\![0, a]\!], \quad v_i = \binom{a}{i}\binom{n-a}{i} \quad , \quad m_i = \binom{n}{i} - \binom{n}{i-1}.$$

The q-numbers of the Johnson schemes involve *Hahn polynomials* H_k^n which are defined as,

$$\forall k \in [\![0,a]\!], \quad H_k^{n,a}(X) \stackrel{\text{def}}{=} m_k \sum_{j\in[\![0,k]\!]} (-1)^j \frac{\binom{k}{j}\binom{n+1-k}{j}}{v_j}\binom{X}{j},$$

where the v_j depend on a. More precisely, the q-numbers are then the integers given by the evaluation of the Hahn polynomials over $[\![0,a]\!]$, *i.e.,*

$$\forall i,k \in [\![0,a]\!], \quad q_k(i) \stackrel{\text{def}}{=} H_k^{n,a}(i). \tag{22}$$

We have in particular,

$$q_1(i) = (n-1)\left(1 - \frac{ni}{a(n-a)}\right) \tag{23}$$

which is a decreasing function as required in Theorems 2 and 3. We consider the linear program associated to this association scheme and we denote $A_{\text{LP}}(n,d,a)$ (as per Subsection 2.6) its maximum value. Let,

$$R_{\text{LP}}(\delta,\alpha) \stackrel{\text{def}}{=} \lim_{n\to\infty} \frac{1}{n}\log_2 A_{\text{LP}}(n,\lfloor n\delta\rfloor,\lfloor n\alpha\rfloor)$$

be its asymptotic value. We have,

$$A(n,d,a) \le A_{\text{LP}}\left(n,\left\lfloor\frac{d}{2}\right\rfloor,a\right) \quad , \quad R(\delta,\alpha) \le R_{\text{LP}}(\delta/2,\alpha).$$

The factor two in the distance comes from the fact that in the association scheme $(\mathcal{S}_a^{n,2},\tau_{\text{J}},a)$, the distance is half of the hamming distance while $A(n,d,a)$ and $R(\delta,\alpha)$ are defined with respect to the Hamming distance.

Hamming Bound. By using the valencies of $(\mathcal{S}_a^{n,2},\tau_{\text{J}},a)$ and Theorem 1 we easily recover the Hamming bound.

Theorem 7 (Hamming Bound for $A_{\text{LP}}(n,d,a)$)**.** *Fix integers n,a,d, where $a \in [\![0,\lfloor n/2\rfloor]\!]$ and $d \in [\![1,n]\!]$. We have,*

$$A_{\text{LP}}(n,d,a) \le \frac{\binom{n}{a}}{\sum_{x=0}^{\lfloor\frac{d-1}{2}\rfloor} v_x} = \frac{\binom{n}{a}}{\sum_{x=0}^{\lfloor\frac{d-1}{2}\rfloor}\binom{a}{x}\binom{n-a}{x}},$$

which implies asymptotically for any $\alpha \in (0,1/2)$ and $\delta \in (0,\alpha(1-\alpha))$,

$$R(2\delta,\alpha) \le R_{\text{LP}}(\delta,\alpha) \le h_2(\alpha) - \left(\alpha h_2\left(\frac{\delta}{2\alpha}\right) + (1-\alpha)h_2\left(\frac{\delta}{2(1-\alpha)}\right)\right).$$

Elias-Bassalygo Bound. We now instantiate to the Hamming sphere $\mathcal{S}_a^{n,2}$ our generalized Elias-Bassalygo bound of Theorem 2. To the best of our knowledge the following upper bound on the linear program was not known.

Theorem 8 (Elias-Bassalygo Bound for $A_{\text{LP}}(n,d,a)$)**.** *Fix integers n,a,d, where $a \in [\![0,\lfloor n/2\rfloor]\!]$ and $d \in [\![0,a(n-a)/n]\!]$. We have,*

$$A_{\text{LP}}(n,d,a) \le (n-1)\frac{nd}{a(n-a)} \cdot \frac{\binom{n}{a}}{\binom{a}{u}\binom{n-a}{u}}, \quad \textit{where} \quad u \stackrel{\textit{def}}{=} \left\lfloor \frac{a(n-a)}{n}\left(1 - \sqrt{1 - \frac{nd}{a(n-a)} + \frac{1}{n-1}}\right)\right\rfloor$$

which implies asymptotically for any $\alpha \in (0,1/2)$ and $\delta \in [0,\alpha(1-\alpha)]$,

$$R(2\delta,\alpha) \le R_{\text{LP}}(\delta,\alpha) \le h_2(\alpha) - \left(\alpha h_2\left(\frac{K(\delta,\alpha)}{\alpha}\right) + (1-\alpha)h_2\left(\frac{K(\delta,\alpha)}{1-\alpha}\right)\right)$$

where $K(\delta,\alpha) \stackrel{\textit{def}}{=} \alpha(1-\alpha)\left(1 - \sqrt{1 - \frac{\delta}{\alpha(1-\alpha)}}\right)$.

Proof. Our strategy is to apply Theorem 2. First q_1 is indeed a decreasing function. Now, let us compute,

$$u \in \left\{ u_0 \in [\![0,n]\!] : \frac{q_1(u_0)^2}{q_1(0)} \geq q_1(d)+1 \right\} \text{ which maximizes } \binom{a}{u}\binom{u}{n-a}.$$

We have,

$$q_1(0)\,(q_1(d)+1) = (n-1)^2\left(1 - \frac{nd}{a(n-a)} + \frac{1}{n-1}\right).$$

Since $d \in [\![0, a(n-a)/n]\!]$, the right hand side is nonnegative and

$$q_1(u_0)^2 \geq q_1(0)\,(q_1(d)+1) \Leftrightarrow 1 - \frac{nu_0}{a(n-a)} \geq \sqrt{1 - \frac{nd}{a(n-a)} + \frac{1}{n-1}}$$

showing that we have to choose u smaller than,

$$\left\lfloor \frac{a(n-a)}{n}\left(1 - \sqrt{1 - \frac{nd}{a(n-a)} + \frac{1}{n-1}}\right)\right\rfloor.$$

We can choose u as above as $y \mapsto \binom{a}{y}\binom{n-a}{y}$ is an increasing function over $\left[\!\!\left[0, \left\lfloor \frac{a(n-a)}{n} \right\rfloor\right]\!\!\right]$. Applying Theorem 2 ends the first part of the proof. The asymptotic result easily follows from Lemma 1. □

MRRW Bound. We end our instantiations by the bound from Theorem 3 to the Johnson scheme. We recover the bound from [MRRW77, Eq. (2.16)].

Theorem 9 (MRRW1-type Bound for $A_{\mathrm{LP}}(n,d,a)$)**.** *Fix integers n, a, d, where $a \in [\![0, \lfloor n/2 \rfloor]\!]$ and $d \in [\![0, a(n-a)/n]\!]$. Let r be an integer such that,*

$$\zeta_r^{(1)} \leq (d-1) < \zeta_{r-1}^{(1)},$$

where $\zeta_x^{(1)}$ is the first zero of $H_r^{n,a}(X)$. We have

$$A_{LP}(n,d,a) \leq (q_1(0) - q_1(d)) \sum_{x=0}^{r-1} m_r,$$

which implies asymptotically for any $\alpha \in [0,1/2]$ and $\delta \in [0, \alpha(1-\alpha)]$,

$$R(2\delta,\alpha) \leq R_{\mathrm{LP}}(\delta,\alpha) \leq h_2(B(\delta,\alpha) \quad \text{with } B(\delta,\alpha) \overset{def}{=} \frac{1}{2}\left(1 - \sqrt{1 - 4\left(\sqrt{\alpha(1-\alpha) - \delta(1-\delta)} - \delta\right)^2}\right).$$

Proof. Fix integers n, d, a. We write $q_1(d-1) - q_1(d) = \frac{n(n-1)}{a(n-a)} \geq 1$ which implies,

$$q_1(d) + 1 \leq q_1(d-1).$$

For each $x \in [\![0,a]\!]$, let $\zeta_x^{(1)} < \zeta_x^{(2)} < \cdots < \zeta_x^{(a)}$ be the zeros of $H_x^{n,a}(X)$ in $[0,a]$. We know that the zeros of $H_x^{n,a}(X)$ and $H_{x+1}^{n,a}(X)$ are interlaced, *i.e.*,

$$\zeta_x^{(i-1)} < \zeta_{x+1}^{(i)} < \zeta_x^{(i)}. \tag{24}$$

Furthermore, we know that there exists an integer in the open interval $(\zeta_{x+1}^{(i)}, \zeta_x^{(i)})$ [MRRW77, §B]. Therefore, by supposing that there exists x such that $\zeta_x^{(1)} < d-1$, we can choose the minimum r such that,

$$\zeta_r^{(1)} \leq (d-1) < \zeta_{r-1}^{(1)} < \zeta_r^{(2)}$$

where in the last inequality we used Equation (24). Let also $r^\perp \overset{\text{def}}{=} d-1$. Since, as shown above $r^\perp < \zeta_r^{(2)}$ we have $H_r^{n,a}(x) \leq 0$ for $x \in [\zeta_r^{(1)}, r^\perp]$ as $H_r^{n,a}(0) = m_r > 0$ and the zeros of $H_r^{n,a}(X)$ are simple. In particular, $q_r(r^\perp) = H_r^{n,a}(r^\perp) \leq 0$. Moreover, we know that $\zeta_x^{(1)} > \zeta_r^{(1)}$ for $x \in [\![0, r-1]\!]$.

Therefore as $H_x^{n,a}(0) = m_x > 0$, we have that for all $x \in [\![0, r-1]\!]$, $q_x(r^\perp) = H_x^{n,a}(r^\perp) \geq 0$. One can therefore use Theorem 3 to obtain,

$$A_{\mathrm{LP}}(n,d,a) \leq (q_1(0) - q_1(d)) \sum_{x=0}^{r-1} m_x.$$

However, we still need to ensure that there exists $x \in [\![0, a]\!]$ such that $\zeta_x^{(1)} < d-1$. To this aim we will use the asymptotic of $\zeta_x^{(1)}$ for n large enough. First, we choose $d \overset{\text{def}}{=} \lfloor \delta n \rfloor$ and $a \overset{\text{def}}{=} \lfloor \alpha n \rfloor$. Let us suppose that $x/n \underset{n \to +\infty}{\longrightarrow} \beta \in [0, \alpha]$. We know from [DL98, §F] that,

$$\frac{\zeta_x}{n} \underset{n\to+\infty}{=} \zeta(\beta) + o(1),$$

where,

$$\zeta(\beta) \overset{\text{def}}{=} \frac{\alpha(1-\alpha) - \beta(1-\beta)}{1 + 2\sqrt{\beta(1-\beta)}}.$$

Furthermore, we know that ζ maps the interval $[0, \alpha]$ onto $[0, \alpha(1-\alpha)]$. We also know that ζ admits an inverse ζ^{-1} that maps $[0, \alpha(1-\alpha)]$ to $[0, \alpha]$ and it is an increasing function. Recall that we supposed $\delta \in [0, \alpha(1-\alpha)]$ where $a = \lfloor \alpha n \rfloor$. Therefore, the minimum r for which we can ensure (for n large enough) $\zeta_r^{(1)} < d-1$ is such that $r/n \underset{n\to+\infty}{\longrightarrow} \beta$ where,

$$\beta = B(\delta, \alpha) \overset{\text{def}}{=} \zeta^{-1}(\delta) = \frac{1}{2}\left(1 - \sqrt{1 - 4\left(\sqrt{\alpha(1-\alpha) - \delta(1-\delta)} - \delta\right)^2}\right).$$

Therefore, when $\delta \in [0, \alpha(1-\alpha)]$, we obtain as asymptotic bound,

$$R_{\mathrm{LP}}(\delta, \alpha) \leq h_2\left(B(\delta, \alpha)\right)$$

which concludes the proof. □

Discussion. We depict in Figure 5 the asymptotic upper bounds over $R(\delta, \alpha)$ obtained in Theorems 7, 8 and 9 for some relative radius α. As it can be noticed the generalized Elias-Bassalygo bounds gives better result than the MRRW-like bound from Theorem 9. It turns out that this result holds for δ close to 0 for any relative radius α. Indeed, we can compute

$$B(\delta, \alpha) \underset{\delta \to 0^+}{=} \alpha - \frac{1 + 2\sqrt{\alpha - \alpha^2}}{1 - 2\alpha}\delta + o(\delta)$$

which gives,

$$R_{\mathrm{MRRW}}(\delta, \alpha) \overset{\text{def}}{=} h_2(B(\delta, \alpha)) \underset{\delta\to 0^+}{=} h_2(\alpha) - \frac{(\log_2(1-\alpha) - \log_2 \alpha)(1 + 2\sqrt{\alpha - \alpha^2})}{1 - 2\alpha}\delta + o(\delta).$$

On the other hand, we have $K(\delta, \alpha) \underset{\delta\to 0^+}{=} \frac{\delta}{2} + o(\delta)$ and $h_2(\delta) \underset{\delta \to 0^+}{=} -\delta \log_2 \delta - o(\delta \log_2 \delta)$ which gives

$$R_{\mathrm{EB}}(\delta, \alpha) \overset{\text{def}}{=} h_2(\alpha) - \alpha h_2\left(\frac{K(\delta, \alpha)}{\alpha}\right) - (1-\alpha) h_2\left(\frac{K(\delta, \alpha)}{1 - \alpha}\right) \underset{\delta \to 0^+}{=} h_2(\alpha) + \delta \log_2(\delta) + o(\delta \log_2(\delta)).$$

One can see here, that $R_{\mathrm{EB}}(\delta, \alpha)$ decreases faster for $\delta \longrightarrow 0^+$ than for the MRRW bound $R_{\mathrm{MRRW}}(\delta, \alpha)$, and this holds for any $\alpha \in (0, \frac{1}{2})$.

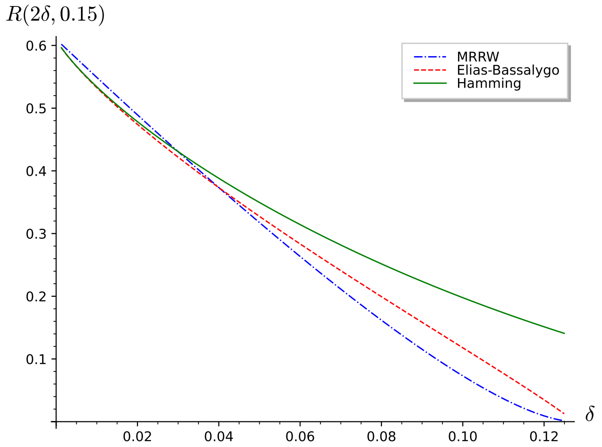

FIGURE 5. Upper bounds on $R_{LP}(\delta, \alpha)$ via the linear program with the Hamming (Theorem 7), Elias-Bassalygo (Theorem 8) and MRRW (Theorem 9) for a relative radius $\alpha = 0.15$.

REFERENCES

[AB06] A. Ashikhmin and A. Barg. Binomial moments of the distance distribution: bounds and applications. *IEEE Trans. Inf. Theor.*, 45(2):438452, sep 2006.

[Bas65] Leonid Alexandrovich Bassalygo. New upper bounds for error correcting codes. *Probl. Peredachi Inf.*, 1:41–44, 1965.

[BI84] Eiichi. Bannai and Tatsuro Ito. *Algebraic combinatorics I : association schemes*. Mathematics lecture note series ; 58. Benjamin/Cummings Pub. Co., Menlo Park, Calif, 1984.

[BJ99] Alexander Barg and David B Jaffe. Numerical results on the asymptotic rate of binary codes. *Codes and Association Schemes*, 56:25–32, 1999.

[CE03] Henry Cohn and Noam Elkies. New upper bounds on sphere packings i. *Annals of mathematics*, pages 689–714, 2003.

[CJJ22] Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones. A Complete Linear Programming Hierarchy for Linear Codes. In *ITCS 2022*, volume 215, pages 51:1–51:22, 2022.

[CJJ23] Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones. Exact Completeness of LP Hierarchies for Linear Codes. In *ITCS 2023*, volume 251, pages 40:1–40:18, 2023.

[CS90] Laura Chihara and Dennis Stanton. Zeros of generalized krawtchouk polynomials. *J. Approx. Theory*, 60(1):4357, jan 1990.

[Del73] Philippe Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep.*, 10, 1973.

[Del94] Ph Delsarte. Application and generalization of the macwilliams transform in coding theory. *Proc. 15th Sympos. Inform. Theory in the Benelux*, 9:44, 1994.

[DL98] Philippe Delsarte and Vladimir Iossifovitch Levenshtein. Association schemes and coding theory. *IEEE Trans. Inform. Theory*, 44(6):2477–2504, 1998.

[FT05] Joel Friedman and Jean-Pierre Tillich. Generalized alon–boppana theorems and error-correcting codes. *SIAM J. Discret. Math.*, 19:700–718, 2005.

[Gil52] E. N. Gilbert. A comparison of signalling alphabets. *Bell System Technical Journal*, 31(3):504–522, 1952.

[KL78] GA Katabiansky and VI Levenshtein. Bounds for packings on a sphere and in space. *Problems of Information Transmission*, 14(1):1–7, 1978.

[LL22] Elyassaf Loyfer and Nati Linial. Linear programming hierarchies in coding theory: Dual solutions. *arXiv preprint arXiv:2211.12977*, 2022.

[LL23] Elyassaf Loyfer and Nati Linial. New LP-based upper bounds in the rate-vs.-distance problem for binary linear codes. *IEEE Trans. Inf. Theor.*, page 28862899, 2023.

[MRRW77] 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. Inform. Theory*, 23(2):157–166, 1977.

[NC10] Michael A Nielsen and Isaac L Chuang. *Quantum computation and quantum information*. Cambridge university press, 2010.

[NS05] M. Navon and A. Samorodnitsky. On delsarte's linear programming bounds for binary codes. In *46th Annual IEEE Symposium on Foundations of Computer Science (FOCS'05)*, pages 327–336, 2005.

[NS07] Michael Navon and Alex Samorodnitsky. Linear programming bounds for codes via a covering argument. *Discrete & Computational Geometry*, 41:199–207, 2007.

[Rod80] ER Rodemich. An inequality in coding theory. In *Papers Presented to the American Mathematical Society*, volume 1, page 15, 1980.

[Sam01] Alex Samorodnitsky. On the optimum of delsarte's linear program. *Journal of Combinatorial Theory, Series A*, 96(2):261–287, 2001.

[Sam23a] Alex Samorodnitsky. On the difficulty to beat the first linear programming bound for binary codes. *arXiv preprint arXiv:2308.16038*, 2023.

[Sam23b] Alex Samorodnitsky. One more proof of the first linear programming bound for binary codes and two conjectures. *Israel Journal of Mathematics*, 256(2):639–673, 2023.

[SGB67] C.E. Shannon, R.G. Gallager, and E.R. Berlekamp. Lower bounds to error probability for coding on discrete memoryless channels. ii. *Information and Control*, 10(5):522–552, 1967.

[Sha48] Claude Elwood Shannon. A mathematical theory of communication. *The Bell System Technical Journal*, 27:379–423, 1948.

[TVZ82] M. A. Tsfasman, S. G. Vldutx, and Th. Zink. Modular curves, shimura curves, and goppa codes, better than varshamov-gilbert bound. *Mathematische Nachrichten*, 109(1):21–28, 1982.

[Var57] Rom Varshamov. Estimate of the number of signals in error correcting codes. *Dokl. Akad. Nauk SSSR*, 117:739–741, 1957.

Appendix A. Proofs on Claimed Results about Association Scheme

Our aim in this appendix is to provide a self-contain section proving all results from Subsections 2.1 to 2.3. We recall here definitions and propositions of these subsections instead of referring to them for ease of reading. Furthermore, we will use Dirac's *bra-ket* notation as introduced in Subsection 2.5.

Recall that where are given (X,τ,n), where X is a finite set and $\tau : \mathsf{X}^2 \longrightarrow [\![0,n]\!]$ is a distance. Furthermore, we consider the following adjacency matrices $\mathbf{D}_i \in \mathbb{C}(\mathsf{X}^2)$ for $i \in [\![0,n]\!]$,

$$\mathbf{D}_i(x,y) \overset{\text{def}}{=} \begin{cases} 1 \text{ if } \tau(x,y) = 1 \\ 0 \text{ otherwise} \end{cases} .$$

In other words,

$$\mathbf{D}_i = \sum_{\substack{x,y\in\mathsf{X} \\ \tau(x,y)=i}} |x\rangle\langle y| \,. \tag{25}$$

We have defined distance induced association schemes as triplets (X,τ,n) satisfying the equipartition and non-degenerate properties which are defined as follows.

Definition 1 (Equipartition Property and Non-Degenerate Triplets)**.** (X,τ,n) *is said to satisfy the equipartition property if for each $i,j,k \in [\![0,n]\!]$, there exists a nonnegative integer $p_{i,j}^k$ such that,*

$$\forall x,z \in \mathsf{X} \text{ such that } \tau(x,z) = k, \quad |\{y \in \mathsf{X} :\ \tau(x,y) = i \text{ and } \tau(y,z) = j\}| = p_{i,j}^k .$$

Furthermore, a triplet (X,τ,n) satisfying the equipartition property is said to be non-degenerate if $p_{1,k}^{k+1} \neq 0$ for all $k \in [\![0,n-1]\!]$.

From the symmetry of τ we easily get the following equation,

$$\forall i,j,k \in [\![0,n]\!], \quad p_{i,j}^k = p_{j,i}^k . \tag{26}$$

The equipartition property ensures that the complex vector space generated by the adjacency matrices $\mathbf{D}_i$ is closed under matrix multiplication, *i.e.,* it forms an associative algebra.

Proposition 1. *Let (X,τ,n) satisfying the equipartition property and let $(\mathbf{D}_i)_{i\in[\![0,n]\!]}$ denote the associated adjacency matrices. We have,*

$$\forall i,j \in [\![0,n]\!], \quad \mathbf{D}_i \cdot \mathbf{D}_j = \sum_{k\in[\![0,n]\!]} p_{i,j}^k \mathbf{D}_k .$$

Proof. According to Equation (25) we have the following computation,

$$\begin{aligned}
\mathbf{D}_i \cdot \mathbf{D}_j &= \sum_{\substack{x,y,x',y'\in\mathsf{X} \\ \tau(x,y)=i \text{ and } \tau(x',y')=j}} |x\rangle\langle y| \cdot |x'\rangle\langle y'| \\
&= \sum_{\substack{x,z,y'\in\mathsf{X} \\ \tau(x,z)=i \text{ and } \tau(z,y')=j}} |x\rangle\langle y'| \\
&= \sum_{k\in[\![0,n]\!]} \sum_{\substack{x,y'\in\mathsf{X} \\ \tau(x,y')=k}} \sum_{\substack{z\in\mathsf{X} \\ \tau(x,z)=i \text{ and } \tau(z,y')=j}} |x\rangle\langle y'| \\
&= \sum_{k\in[\![0,n]\!]} \sum_{\substack{x,y'\in\mathsf{X} \\ \tau(x,y')=k}} p_{i,j}^k \, |x\rangle\langle y'|
\end{aligned}$$

where in the last equality we used the definition of the $p_{i,j}^k$ given in Definition 1. To conclude the proof it remains to use Equation (25). □

We are now ready to properly define distance induced association schemes.

Definition 2. *A distance induced association scheme is a triplet* (X, τ, n) *where* X *is a finite set,* $\tau : \mathsf{X}^2 \longrightarrow [\![0, n]\!]$ *is a distance and* (X, τ, n) *satisfies the equipartition property and is non-degenerate.*

A.1. **Polynomial Relations.** According to Proposition 1 and Equation (26), the associated matrices $\mathbf{D}_i$'s from a given association scheme (X, τ, n) commute. Therefore these adjacency matrices (over $\mathbb{C}$) are diagonalizable in the same basis (they are all diagonalizable as $\mathbf{D}_i^\dagger = \mathbf{D}_i$ by symmetry of the distance τ). We can actually prove that they also share the same eigenspaces.

Notice that τ is ranging over $[\![0, n]\!]$ and it satisfies the triangular inequality (it is a distance) from which we deduce the crucial equation,

$$p_{i,j}^k = 0 \text{ if } k > i + j, \text{ or } |j - i| > k \text{ or as soon as } i, j, k > n. \tag{27}$$

Notice that together with Proposition 1 it implies the fundamental relation,

$$\forall k \in [\![0, n]\!], \quad \mathbf{D}_1 \mathbf{D}_k = p_{1,k}^{k-1} \mathbf{D}_{k-1} + p_{1,k}^k \mathbf{D}_k + p_{1,k}^{k+1} \mathbf{D}_{k+1}. \tag{28}$$

But, as (X, τ, n) is non-degenerate, *i.e.*, $p_{1,k}^{k+1} \neq 0$,

$$\mathbf{D}_{k+1} = \frac{1}{p_{1,k}^{k+1}} \left(\mathbf{D}_1 \mathbf{D}_k - p_{1,k}^{k-1} \mathbf{D}_{k-1} - p_{1,k}^k \mathbf{D}_k \right). \tag{29}$$

In particular, $\mathbf{D}_2$ is some polynomial of degree 1 in $\mathbf{D}_1$ ($\mathbf{D}_0$ is the identity matrix). We can then extend this result to the other $\mathbf{D}_i$'s as shown in the following proposition.

Proposition 14. *Let* (X, τ, n) *be a distance induced association scheme with adjacency matrices* $(\mathbf{D}_i)_{i \in [\![0,n]\!]}$. *Then, for all* $i \in [\![0, n]\!]$, *there exists a polynomial* $P_i \in \mathbb{R}[X]$ *of degree* i *with leading coefficient* $\left(\prod_{j=1}^{i-1} p_{1,j}^{j+1} \right)^{-1}$ *such that*

$$\mathbf{D}_i = P_i(\mathbf{D}_1)$$

We call these polynomials the fundamental P*-polynomials of the association scheme* (X, τ, n).

Proof. This proposition follows from a straightforward induction using Equation (29) and the fact that (X, τ, n) is non-degenerate. □

A.2. **Eigenstates and Eigenvalues of the $\mathbf{D}_i$'s: Introducing the $\mathbf{E}_i$'s.** The polynomial relation from Proposition 14 shows that the $\mathbf{D}_i$'s share common eigenspaces in addition to be co-diagonalizable. Furthermore, combining this result with Proposition 1 (in particular Equation (27)) shows that the $\mathbf{D}_i$'s can be decomposed as the sum of $n + 1$ orthogonal projectors.

Proposition 15. *Let* (X, τ, n) *be a distance induced association scheme with associated adjacency matrices* $(\mathbf{D}_i)_{i \in [\![0,n]\!]}$. *There exist orthogonal projectors* $(\mathbf{E}_i)_{i \in [\![0,n]\!]}$ *and distinct* $(\lambda_i)_{i \in [\![0,n]\!]} \in \mathbb{R}^{n+1}$ *such that,*

$$\forall i \in [\![0, n]\!], \quad \mathbf{D}_i = \sum_{j \in [\![0,n]\!]} P_i(\lambda_j) \mathbf{E}_j$$

where the P_i*'s are the fundamental* P*-polynomials of the association scheme* (X, τ, n).

Furthermore, one can choose

$$\mathbf{E}_0 = \frac{1}{|\mathsf{X}|} \sum_{x, y \in [\![0,n]\!]} |x\rangle\langle y|.$$

Proof. First, $\mathbf{D}_1$ is diagonalizable because $\mathbf{D}_1^\dagger = \mathbf{D}_1$ and its eigenvalues are real. Therefore there exist real numbers $\lambda_0 > \lambda_1 > \cdots > \lambda_m$ and orthogonal projectors $\mathbf{E}_0, \ldots, \mathbf{E}_m$ such that,

$$\mathbf{D}_1 = \sum_{j \in [\![0,m]\!]} \lambda_j \mathbf{E}_j. \tag{30}$$

From Proposition 14 we deduce that (notice that $\mathbf{E}_j^2 = \mathbf{E}_j$ and $\mathbf{E}_i\mathbf{E}_j = \mathbf{0}$ for $i \neq j$),

$$\forall i \in [\![0,n]\!], \quad \mathbf{D}_i = P_i(\mathbf{D}_1) = \sum_{j \in [\![0,m]\!]} P_i(\lambda_j)\mathbf{E}_j \tag{31}$$

where the P_i's are the fundamental P-polynomials. They have degree i and leading coefficient $\left(\prod_{j=1}^{i-1} p_{1,j}^{j+1}\right)^{-1}$. Let us show that $m = n$ to conclude the proof.

First, $m \geq n$. Indeed, by the decomposition from Proposition 1 and using Equation (27) we get,

$$\mathbf{D}_1\mathbf{D}_n = p_{1,n}^{n-1}\mathbf{D}_{n-1} + p_{1,n}^{n}\mathbf{D}_n. \tag{32}$$

Let,

$$Q \stackrel{\text{def}}{=} P_1 P_n - p_{1,n}^{n-1}P_{n-1} - p_{1,n}^{n}P_n \in \mathbb{R}[X].$$

This polynomial has degree $\leq n+1$. Furthermore, plugging $\mathbf{D}_n = P_n(\mathbf{D}_1)$ and $\mathbf{D}_1 = P_1(\mathbf{D}_1)$ into Equation (32) shows that $Q(\mathbf{D}_1) = 0$. Therefore, from the fact that the $\mathbf{E}_i$'s are orthogonal projectors and Equation (30),

$$\forall i \in [\![0,m]\!], \quad Q(\lambda_i) = 0.$$

But the degree of Q is $\leq n+1$ showing that $m \leq n$. Let us show now that $n \leq m$. Assume by contradiction that $m < n$. Let $R(X) \stackrel{\text{def}}{=} \prod_{i=0}^{m}(X - \lambda_i)$. By Equation (30),

$$R(\mathbf{D}_1) = \mathbf{0}.$$

By writing $R(X) = X^m + \sum_{j=0}^{m-1} a_j X^j$, we obtain

$$R(\mathbf{D}_1) = \mathbf{D}_1^m + \sum_{j=0}^{m-1} a_j \mathbf{D}_1^j.$$

By definition, P_m has leading coefficient $\left(\prod_{j=1}^{m-1} p_{1,j}^{j+1}\right)^{-1}$. Therefore, by using $\mathbf{D}_m = P_m(\mathbf{D}_1)$ (see Equation (31)) with the fact that the $\mathbf{E}_j$'s are orthogonal projectors, we obtain for some b_j's,

$$R(\mathbf{D}_1) = \left(\prod_{j=1}^{m-1} p_{1,j}^{j+1}\right)\mathbf{D}_m + \sum_{j=0}^{m-1} b_j \mathbf{D}_j.$$

It shows $R(\mathbf{D}_1) \neq \mathbf{0}$ which is a contradiction. Indeed, (X, τ, n) is non-degenerate: by definition the $p_{1,j}^{j+1}$'s are non-zero.

To conclude the proof let us show (up to a re-ordering) that we have,

$$\mathbf{E}_0 = \frac{1}{|\mathsf{X}|}\sum_{x,y \in X} |x\rangle\langle y| = \frac{1}{|\mathsf{X}|}\mathbf{J}.$$

First, notice that $\mathbf{J} = \sum_{i \in [\![0,n]\!]} \mathbf{D}_i$. Therefore, $\mathbf{J}$ belongs to the space generated by the $\mathbf{D}_i$'s which is also generated by the $\mathbf{E}_i$'s. It shows that we can write $\mathbf{J} = \sum_{i \in [\![0,n]\!]} \beta_i \mathbf{E}_i$ and we can suppose that $\beta_0 \neq 0$. As the $\mathbf{E}_i$'s are orthogonal projectors we get,

$$\mathbf{E}_0 = \frac{1}{\beta_0}\mathbf{J}\mathbf{E}_0 = \mathbf{E}_0\mathbf{J}. \tag{33}$$

In particular $\mathbf{E}_0$ and $\mathbf{J}$ commute. On the other hand, as $\mathbf{J}^2 = |\mathsf{X}|\,\mathbf{J}$, we also have,

$$\mathbf{J}\mathbf{E}_0 = \frac{1}{|\mathsf{X}|}\mathbf{J}^2\mathbf{E}_0 = \frac{1}{|\mathsf{X}|}\mathbf{J}\left(\mathbf{E}_0\mathbf{J}\right) = \frac{\beta}{|\mathsf{X}|}\mathbf{J}$$

where β is the sum of all the entries of $\mathbf{E}_0$. We deduce by combining the above equation and Equation (33) that $\mathbf{E}_0$ is a scalar multiple of $\mathbf{J}$. Using now that $\mathbf{E}_0^2 = \mathbf{E}_0$ shows that $\mathbf{E}_0 = 1/|\mathsf{X}|\mathbf{J}$ which concludes the proof. □

The fundamental parameters of an association scheme are defined with respect to an ordering of the matrices $(\mathbf{E}_i)_{i \in [\![0,n]\!]}$. In what follows we will only enforce an ordering such that, $\mathbf{E}_0 = 1/|\mathsf{X}| \sum_{x,y \in [\![0,n]\!]} |x\rangle\langle y|$ which is possible as shown in the above proposition.

Definition 3 (p-numbers)**.** *Let (X,τ,n) be a distance induced association scheme with an ordering $\mathbf{E}_0,\dots,\mathbf{E}_n$. Its underlying p-numbers $p_i(j)$ are defined as,*

$$\forall i \in [\![0,n]\!], \quad \mathbf{D}_i = \sum_{j\in[\![0,n]\!]} p_i(j)\mathbf{E}_j.$$

Remark 5. *The matrices $\mathbf{E}_i$'s are the orthogonal projectors over the (common) eigenspaces of the adjacency matrices $\mathbf{D}_i$'s. Therefore they sum to the identity, i.e., $\sum_{i\in[\![0,n]\!]}\mathbf{E}_i = \mathbf{Id}$. But $\mathbf{D}_0 = \mathbf{Id}$ which shows from the decomposition in Definition 3 that,*

$$\forall j \in [\![0,n]\!], \quad p_0(j) = 1. \tag{34}$$

The p-numbers are well defined as matrices $(\mathbf{D}_i)_{i\in[\![0,n]\!]}$ and $(\mathbf{E}_i)_{i\in[\![0,n]\!]}$ generate the same Hilbert space of dimension $n+1$.

Proposition 16. *We have,*

$$p_1(j)p_i(j) = p_{1,i}^{i-1}p_{i-1}(j) + p_{1,i}^{i}p_i(j) + p_{1,i}^{i+1}p_{i+1}(j)$$

Proof. First, by using Definition 3,

$$\mathbf{D}_1\cdot\mathbf{D}_i = \sum_{j,\ell\in[\![0,n]\!]} p_1(j)p_i(\ell)\mathbf{E}_i\cdot\mathbf{E}_\ell = \sum_{j\in[\![0,n]\!]} p_1(j)p_i(j)\mathbf{E}_j$$

where we used in the last equality that $\mathbf{E}_i\cdot\mathbf{E}_j = \delta_i^j\cdot\mathbf{E}_i$ as orthogonal projectors. Recall now that from Equation (28),

$$\begin{aligned}\forall j \in [\![0,n]\!], \quad \mathbf{D}_1\mathbf{D}_i &= p_{1,i}^{i-1}\mathbf{D}_{i-1} + p_{1,i}^{i}\mathbf{D}_i + p_{1,i}^{i+1}\mathbf{D}_{i+1}\\ &= \sum_{j\in[\![0,n]\!]}\left(p_{1,i}^{i-1}p_{i-1}(j) + p_{1,i}^{i}p_i(j) + p_{1,i}^{i+1}p_{i+1}(j)\right)\mathbf{E}_j.\end{aligned}$$

It ends the proof by using the unicity of the decomposition given in the basis $(\mathbf{E}_i)_{i\in[\![0,n]\!]}$. □

The fact that the $(\mathbf{D}_i)_{i\in[\![0,n]\!]}$ and $(\mathbf{E}_i)_{i\in[\![0,n]\!]}$ generate the same Hilbert enables to define the q-numbers, an equivalent of the p-numbers (according to Definition 3), where the $\mathbf{E}_i$'s and $\mathbf{D}_i$'s are interchanged.

Definition 5 (q-numbers)**.** *Let (X,τ,n) be a distance induced association scheme with an ordering $\mathbf{E}_0,\dots,\mathbf{E}_n$. Its underlying q-numbers $q_i(j)$ are defined from the expansion of the orthogonal projectors $\mathbf{E}_i$ in the basis of adjacency matrices $(\mathbf{D}_j)_{j\in[\![0,n]\!]}$, i.e.,*

$$\forall i \in [\![0,n]\!], \quad \mathbf{E}_i = \frac{1}{|\mathsf{X}|}\sum_{j\in[\![0,n]\!]} q_i(j)\mathbf{D}_j.$$

Notice that the q-numbers are uniquely defined as for p-numbers and they are real numbers as $\mathbf{E}_i^\dagger = \mathbf{E}_i$ and $\mathbf{D}_i^\dagger = \mathbf{D}_i$.

Remark 6. *In Proposition 15 we chose an ordering such that*

$$\mathbf{E}_0 = \frac{1}{|\mathsf{X}|}\sum_{x,y\in[\![0,n]\!]} |x\rangle\langle y|. \tag{35}$$

Here the $\mathbf{D}_j$'s are adjacency matrices associated to a metric. In particular they sum to $|\mathsf{X}|\cdot\mathbf{E}_0$. Therefore it is necessary that,

$$\forall j \in [\![0,n]\!], \quad q_0(j) = 1.$$

It may be tempting to conjecture that the q-numbers verify also a 3-term order recurrence as the one given for the p-numbers in Proposition 16. It will turn out that such relation is crucial for our purpose. However, we first need to define an equivalent of the $p_{i,j}^{\ell}$'s: the $q_{i,j}^{\ell}$'s. There will be defined in Subsection A.4 and they are known as *Krein parameters*. To this aim let us study the orthogonality relations of the $\mathbf{D}_i$'s and $\mathbf{E}_i$'s.

A.3. **Orthogonality Relations.** It turns out (by symmetry of the underlying distance τ) that the $\mathbf{D}_i$'s are orthogonal, *i.e.,* $\langle \mathbf{D}_i | \mathbf{D}_j \rangle = 0$, but also the $\mathbf{E}_i$'s, *i.e.,* $\langle \mathbf{E}_i | \mathbf{E}_j \rangle = 0$, as orthogonal projectors.

Recall that we have defined their norms (with a normalization) as follows.

Definition 4. *Let* (X, τ, n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0, \ldots, \mathbf{E}_n$*, we define,*

$$\forall i \in [\![0,n]\!], \quad v_i \overset{def}{=} \frac{\|\mathbf{D}_i\|^2}{|\mathsf{X}|} \quad \textit{and} \quad m_i \overset{def}{=} \|\mathbf{E}_i\|^2 = \operatorname{rank}(\mathbf{E}_i).$$

The p and q-numbers were derived from matrices $\mathbf{D}_i$'s and $\mathbf{E}_i$'s. They satisfy the following "orthogonality" relations.

Proposition 17. *For any* $i, j \in [\![0,n]\!]$*,*

$$\sum_{k \in [\![0,n]\!]} p_i(k) p_j(k) m_k = \delta_i^j \cdot v_i \cdot |\mathsf{X}| \quad \textit{and} \quad \sum_{k \in [\![0,n]\!]} q_i(k) q_j(k) v_k = \delta_i^j \cdot m_i \cdot |\mathsf{X}|$$

Proof. We just have to use Definitions 3, 5 and the orthogonality of the $\mathbf{D}_i$'s and $\mathbf{E}_j$'s. □

Furthermore, p and q-numbers are related as follows.

Proposition 2. *Let* (X, τ, n) *be a distance induced association scheme with an ordering* $\mathbf{E}_0, \ldots, \mathbf{E}_n$*.*

$$\forall i, j \in [\![0,n]\!], \quad m_j p_i(j) = v_i q_j(i).$$

Proof. First, by Definition 3 and orthogonality of the $\mathbf{E}_j$'s,

$$\forall j \in [\![0,n]\!], \quad \langle \mathbf{D}_i | \mathbf{E}_j \rangle = p_i(j) \|\mathbf{E}_j\|^2 = p_i(j) m_j \quad \text{and} \quad \langle \mathbf{E}_j | \mathbf{D}_i \rangle = \frac{1}{|\mathsf{X}|} q_j(i) \|\mathbf{D}_i\|^2 = q_j(i) v_i. \tag{36}$$

To end the proof we just have to use the fact that $\langle \mathbf{A} | \mathbf{B} \rangle = \overline{\langle \mathbf{B} | \mathbf{A} \rangle}$ and that the $p_i(j)$'s and $q_i(j)$'s are real numbers. □

A.4. **Algebra Structure for Pointwise Multiplication.** In the above subsections we investigated the structure of distance induced association schemes via the complex complex commutative algebra $\mathcal{H}$ generated by its underlying adjacency matrices $\mathbf{D}_i$'s. As we have shown, it turns out that $\mathcal{H}$ is also generated by matrices $\mathbf{E}_i$'s which are orthogonal as the $\mathbf{D}_i$'s. However, though $\mathcal{H}$ forms a an algebra for the standard matrix-product, it is also (surprisingly) closed under the pointwise multiplication $(\mathbf{M}, \mathbf{N}) \mapsto \mathbf{M} \circ \mathbf{N}$ where,

$$\mathbf{M} \circ \mathbf{N}(x,y) = \mathbf{M}(x,y) \mathbf{N}(x,y).$$

Indeed the $\mathbf{D}_i$'s verify the following relation

$$\mathbf{D}_i \circ \mathbf{D}_j = \delta_i^j \cdot \mathbf{D}_i \tag{37}$$

and we have the following proposition which in particular gives an equivalent of the $p_{i,j}^{\ell}$'s.

Proposition 18. *We have,*

$$|\mathsf{X}| \cdot \mathbf{E}_i \circ \mathbf{E}_j = \sum_{k \in [\![0,n]\!]} q_{i,j}^k \mathbf{E}_k, \quad \textit{where } q_{i,j}^k \overset{def}{=} \frac{1}{|\mathsf{X}|} \sum_{m \in [\![0,n]\!]} q_i(m) q_j(m) p_m(k).$$

Proof. First,

$$\begin{aligned}
\mathbf{E}_i \circ \mathbf{E}_j &= \sum_{x,y \in [\![0,n]\!]} \langle x|\, \mathbf{E}_i \,|y\rangle \, \langle x|\, \mathbf{E}_j \,|y\rangle \, |x\rangle\!\langle y| \\
&= \frac{1}{|\mathsf{X}|^2} \sum_{x,y \in [\![0,n]\!]} \left(\sum_{k \in [\![0,n]\!]} \langle x|\, q_i(k)\mathbf{D}_k \,|y\rangle \right) \left(\sum_{\ell \in [\![0,n]\!]} \langle x|\, q_j(\ell)\mathbf{D}_\ell \,|y\rangle \right) |x\rangle\!\langle y| \quad \text{(By Definition 5)} \\
&= \frac{1}{|\mathsf{X}|^2} \sum_{m \in [\![0,n]\!]} \sum_{\substack{x,y \in [\![0,n]\!] \\ \tau(x,y)=m}} q_i(m)q_j(m) \, |x\rangle\!\langle y|
\end{aligned}$$

Therefore,

$$\mathbf{E}_i \circ \mathbf{E}_j = \frac{1}{|\mathsf{X}|^2} \sum_{m \in [\![0,n]\!]} q_i(m)q_j(m)\mathbf{D}_m = \frac{1}{|\mathsf{X}|^2} \sum_{m,\ell \in [\![0,n]\!]} q_i(m)q_j(m)p_m(\ell)\mathbf{E}_\ell$$

which concludes the proof. □

The numbers $q_{i,j}^k$'s are analogous to the $p_{i,j}^k$'s but when decomposing in the basis given by the $\mathbf{E}_i$'s and considering the pointwise multiplication. It turns out that the $q_{i,j}^k$'s are known as the *Krein parameters* of the underlying association scheme and they indeed share the same kind of property. It is readily verified that from Proposition 18 that the $q_{i,j}^\ell$'s are symmetric, *i.e.,*

$$\forall i,j,k \in [\![0,n]\!], \quad q_{i,j}^k = q_{j,i}^k.$$

Furthermore, Krein parameters verify numerous relations. In the following proposition we give some of them which are useful four our purpose.

Proposition 19. *Let (X,τ,n) be a distance induced association scheme with an ordering $\mathbf{E}_0,\dots,\mathbf{E}_n$. We have, for all $x,y \in [\![0,n]\!]$,*

$$(1)\ \ q_{x,x}^0 = m_x > 0 \quad , \quad (2) \sum_{y \in [\![0,n]\!]} q_{y,1}^x = q_1(0) \quad , \quad (3)\ \ m_x \cdot q_{y,1}^x = m_y \cdot q_{x,1}^y.$$

Proof. Let us first prove (1). By Proposition 18,

$$\begin{aligned}
q_{x,x}^0 &= \frac{1}{|\mathsf{X}|} \sum_{m \in [\![0,n]\!]} q_x(m)q_x(m)p_m(0) \\
&= \frac{1}{|\mathsf{X}|} \sum_{m \in [\![0,n]\!]} q_x(m)q_x(m)\frac{v_m}{m_0}q_0(m) \quad \text{(By Proposition 2)} \\
&= \frac{1}{|\mathsf{X}|} \sum_{m \in [\![0,n]\!]} q_x(m)q_x(m)v_m \quad (m_0 = \mathrm{rank}(\mathbf{E}_0) = 1 \text{ by Equation (35)}) \\
&= m_x
\end{aligned}$$

where in the last equality we used Proposition 17. We prove now (2). First, according to Proposition 18,

$$\begin{aligned}
\sum_{y\in\llbracket 0,n\rrbracket} q^{x}_{y,1} &= \sum_{y,m\in\llbracket 0,n\rrbracket} q_1(m)q_y(m)p_m(x) \\
&= \sum_{m\in\llbracket 0,n\rrbracket} q_1(m)p_m(x)\,\frac{1}{v_m}\left(\sum_{y\in\llbracket 0,n\rrbracket} m_y p_m(y)\right) \\
&= \sum_{m\in\llbracket 0,n\rrbracket} q_1(m)p_m(x)\,\frac{1}{v_m}\left(\sum_{y\in\llbracket 0,n\rrbracket} m_y p_m(y)p_0(y)\right) \qquad \text{(By Equation (34))} \\
&= \sum_{m\in\llbracket 0,n\rrbracket} q_1(m)p_m(x)\,\frac{\delta_0^m v_m}{v_m} \qquad \text{(By Proposition 17)} \\
&= q_1(0)
\end{aligned}$$

where in the last equality we used that p_0 is constant and equal to 1 as shown in Equation (34). Let us now finish the proof by proving (3). According once again to Proposition 18,

$$q^{y}_{x,1} = \sum_{m\in\llbracket 0,n\rrbracket} q_1(m)q_x(m)p_m(y).$$

Therefore, according to Proposition 2,

$$q^{y}_{x,1} = \sum_{m\in[0,n]} q_1(m)\; p_m(x)\frac{m_x}{v_m}\; q_y(m)\frac{v_m}{m_y} = \frac{m_x}{m_y}\; q^{x}_{y,1}$$

which ends the proof. □

More surprisingly, Krein parameters are also positive (which is crucial for our purpose, in particular to prove Proposition 6) as shown in the following proposition.

Proposition 3. $\forall i,j,k \in \llbracket 0,n\rrbracket, \quad q^{k}_{i,j} \geq 0.$

Proof. Let $|\psi\rangle \in \mathbb{C}(\mathsf{X})$. Let us introduce the following linear operator,

$$\Delta \overset{\text{def}}{=} \sum_{x\in\mathsf{X}} \langle\psi|x\rangle\, |x\rangle\langle x|$$

We have the following computation,

$$\begin{aligned}
\|\mathbf{E}_i\Delta\mathbf{E}_j\|^2 = \operatorname{tr}\left(\Delta^{\dagger}\mathbf{E}_i\Delta\mathbf{E}_j\right) &= \sum_{y\in\mathsf{X}} \langle y|\,\Delta^{\dagger}\mathbf{E}_i\Delta\mathbf{E}_j\,|y\rangle \\
&= \sum_{y\in\mathsf{X}} \overline{\langle\psi|y\rangle}\,\langle y|\,\mathbf{E}_i\left(\sum_{x\in\mathsf{X}}\langle\psi|x\rangle\,|x\rangle\langle x|\right)\mathbf{E}_j\,|y\rangle \\
&= \sum_{y,x\in\mathsf{X}} \overline{\langle\psi|y\rangle}\,\langle\psi|x\rangle\,\mathbf{E}_i(y,x)\mathbf{E}_j(x,y) \\
&= \sum_{y,x\in\mathsf{X}} \overline{\langle\psi|y\rangle}\,\langle\psi|x\rangle\,\mathbf{E}_i(x,y)\mathbf{E}_j(x,y) \qquad \left(\mathbf{E}_i^{\dagger} = \mathbf{E}_i \text{ and } \mathbf{E}_i \text{ is real}\right) \\
&= \sum_{k\in\llbracket 0,n\rrbracket}\sum_{y,x\in\mathsf{X}} q^{k}_{i,j}\overline{\langle\psi|y\rangle}\,\langle\psi|x\rangle\,\mathbf{E}_k(x,y) \qquad (38)
\end{aligned}$$

Furthermore, we have,

$$\|\mathbf{E}_k\,|\psi\rangle\,\|^2 = \langle\psi|\,\mathbf{E}_k\,|\psi\rangle = \langle\psi|\left(\sum_{x,y\in\mathsf{X}}\mathbf{E}_k(x,y)\,|x\rangle\langle y|\right)|\psi\rangle = \sum_{y,x\in\mathsf{X}} q^{k}_{i,j}\overline{\langle\psi|y\rangle}\,\langle\psi|x\rangle\,\mathbf{E}_k(x,y)$$

Plugging this into Equation (38) shows that,

$$\|\mathbf{E}_i\Delta\mathbf{E}_j\|^2 = \sum_{k\in\llbracket 0,n\rrbracket} q^{k}_{i,j}\,\|\mathbf{E}_k\,|\psi\rangle\,\|^2$$

Given $k_0 \in [\![0,n]\!]$, we choose $|\psi\rangle$ such that $\mathbf{E}_{k_0}|\psi\rangle \neq \mathbf{0}$ and $\mathbf{E}_k|\psi\rangle = \mathbf{0}$. It is possible since the $\mathbf{E}_i$'s are orthogonal projectors. Plugging such $|\psi\rangle$ in the above equation shows that,

$$\|\mathbf{E}_i \Delta \mathbf{E}_j\|^2 = q_{i,j}^{k_0} \|\mathbf{E}_{k_0}|\psi\rangle\|^2 \geq 0$$

where $i,j,k_0 \in [\![0,n]\!]$ are arbitrary. It concludes the proof. □

Krein parameters also appear when considering the product of q-numbers.

Proposition 4. $\forall i,k,\ell \in [\![0,n]\!], \quad q_k(i)q_\ell(i) = \sum_{m\in[\![0,n]\!]} q_{k,\ell}^m q_m(i)$.

Proof. By Definition 5 Equation (37) and orthogonality of the $\mathbf{D}_i$'s whose square norm is v_i,

$$q_k(i)q_\ell(i) = \frac{1}{\|\mathbf{D}_i\|^2}\langle |\mathsf{X}| \cdot \mathbf{E}_i \circ |\mathsf{X}| \cdot \mathbf{E}_\ell, \mathbf{D}_i\rangle = \frac{1}{|\mathsf{X}| \cdot v_i}\langle |\mathsf{X}| \cdot \mathbf{E}_i \circ |\mathsf{X}| \cdot \mathbf{E}_\ell, \mathbf{D}_i\rangle$$

Now using Proposition 18,

$$q_k(i)q_\ell(i) = \frac{1}{v_i}\sum_{m\in[\![0,n]\!]} q_{k,\ell}^m \langle \mathbf{E}_m, \mathbf{D}_i\rangle = \frac{1}{v_i}\sum_{k\in[\![0,n]\!]} q_{k,\ell}^m \, v_i \, q_m(i)$$

where in the last equality we used Equation (36). It concludes the proof. □

Inria de Paris, Paris 75012

Email address: andre.chailloux@inria.fr

Inria Saclay, Palaiseau 91120

Email address: thomas.debris@inria.fr