Higher-order Delsarte Dual LPs: Lifting, Constructions and Completeness

Leonardo Nagami Coregliano[*] Fernando Granha Jeronimo[†] Chris Jones[‡]
Nati Linial[§] Elyassaf Loyfer[¶]

December 8, 2024

Abstract

A central and longstanding open problem in coding theory is the rate-versus-distance trade-off for binary error-correcting codes. In a seminal work, Delsarte introduced a family of linear programs establishing relaxations on the size of optimum codes. To date, the state-of-the-art upper bounds for binary codes come from dual feasible solutions to these LPs. Still, these bounds are exponentially far from the best-known existential constructions.

Recently, hierarchies of linear programs extending and strengthening Delsarte's original LPs were introduced for linear codes, which we refer to as higher-order Delsarte LPs. These new hierarchies were shown to provably converge to the actual value of optimum codes, namely, they are complete hierarchies. Therefore, understanding them and their dual formulations becomes a valuable line of investigation. Nonetheless, their higher-order structure poses challenges. In fact, analysis of all known convex programming hierarchies strengthening Delsarte's original LPs has turned out to be exceedingly difficult and essentially nothing is known, stalling progress in the area since the 1970s.

Our main result is an analysis of the higher-order Delsarte LPs via their dual formulation. Although quantitatively, our current analysis only matches the best-known upper bounds, it shows, for the first time, how to tame the complexity of analyzing a hierarchy strengthening Delsarte's original LPs. In doing so, we reach a better understanding of the structure of the hierarchy, which may serve as the foundation for further quantitative improvements. We provide two additional structural results for this hierarchy. First, we show how to *explicitly* lift any feasible dual solution from level k to a (suitable) larger level ℓ while retaining the objective value. Second, we give a novel proof of completeness using the dual formulation.

[*] University of Chicago. lenacore@uchicago.edu.

[†] University of Illinois Urbana-Champaign. granha@illinois.edu.

[‡] Bocconi University. chris.jones@unibocconi.it.

[§] The Hebrew University of Jerusalem. nati@cs.huji.ac.il. Supported in part by Advanced ERC Grant PaDiDom 101141253.

[¶] The Hebrew University of Jerusalem. elyassaf.loyfer@mail.huji.ac.il

Contents

1 Introduction

A central and longstanding open problem in coding theory is the rate-vs-distance tradeoff for binary error-correcting codes. Roughly speaking, it asks for every $\delta \in (0, 1/2)$, what is the largest exponent $R_2(\delta)$ such that there is a distance δn error-correcting code of size $2^{R_2(\delta)n}$? Despite many decades of effort, the best upper and lower bounds on the rate $R_2(\delta)$ are still far apart, implying that we do not understand the exponential growth rate of optimal binary codes.

Convex programming is not only fundamental to algorithm design but it can also be employed to study combinatorial and mathematical structures. The best known upper bounds on $R_2(\delta)$ come from the analysis of convex programming relaxations. In a seminal work, Delsarte [Del73] showed how to set up linear program relaxations for the maximum possible size of an error-correcting code. The Delsarte LPs have unfolded into a far-reaching theory leading, for instance, to the best known upper bounds on $R_2(\delta)$ [MRRW77], to breakthroughs in sphere packing [CE03, Via17, CKM$^+$17], and to improved bounds on packings and codes in other types of geometric spaces [Lev98, Bac06, BV08, BN06].

The success of convex relaxations is sometimes limited by an *integrality gap* between their optimum and the true value of the combinatorial problem. For error-correcting codes, it is known that the value of the Delsarte LP is exponentially far from the Gilbert–Varshamov lower bound [Sam01]. If the true size of an optimal binary code is actually near the Gilbert–Varshamov bound (as conjectured by some specialists [JV04, Gop93]), then this family of relaxations needs to be substantially strengthened.

Given this context, stronger convex relaxations might be imperative to tighten the upper bounds. In principle, powerful semi-definite programming (SDP) tools such as the Sum-of-Squares hierarchy [Las15] can be applied to this problem [Lau07]. However, asymptotic analysis of these SDP-based relaxations remains elusive even for the simplest cases [Sch05], and only numerical results are known for small constant values of blocklength [GMS12].

To appreciate the difficulty of asymptotically analyzing convex relaxations, recall that the goal is to construct a feasible dual solution which upper bounds the primal objective value. Typically, this requires an explicit construction and analysis. This is a different goal from typical uses of convex programming in algorithm design, where the starting point of the analysis is a solution returned by a convex programming solver. There, one does not need to know the precise structure of the optimum but only the property that it is (near) optimum.

Recently, hierarchies of linear programs extending the Delsarte LPs were proposed for the important case of linear codes [CJJ22, LL23b]. We refer to them informally as "higher-order Delsarte LPs". The idea behind them is to strengthen the Delsarte LPs with additional natural constraints which nonetheless might be simple enough to theoretically analyze. In fact, these hierarchies were shown to converge to the true size of the code [CJJ22, CJJ23], namely, they are complete. Besides being LPs instead of SDPs, these hierarchies bear strong similarities with Delsarte LPs for which we now have various theoretical analyses and a richer set of techniques [MRRW77, FT05, NS05, BN06, BN08, NS09, Sam23b, LL23a, CDA24].

Constructing dual solutions for the higher-order Delsarte LPs can lead to a breakthrough in the rate-versus-distance problem. Nonetheless, the higher-order structure of these LPs may still require substantial effort to be understood and analyzed. In this work, our main goal is to substantially increase our understanding of the structure of the higher-order Delsarte LP hierarchies by establishing three new results about their dual formulations.

Before we present our results, we first recall these LPs with an informal and intuitive description (see Section 2 and Appendix A for more details). The Delsarte LP (used in the first LP bound) has a variable intended to count the number of codewords of each Hamming weight. The higher-order Delsarte LPs form a hierarchy with a level parameter $\ell \in \mathbb{N}$. There is a variable intended to count the number of ℓ-tuples of codewords with every possible Hamming weight configuration of a subspace of dimension ℓ. For example, for $\ell = 2$, essentially there is a variable for each $(a, b, c) \in \{0, 1, \dots, n\}^3$ which is intended to be the number of pairs of codewords (x, y) such that $(|x|, |y|, |x + y|) = (a, b, c)$.

1.1 Our Contributions

We show three different ways of constructing dual solutions for the higher-order Delsarte LPs. First, we show how to lift a solution from any level k to a higher level ℓ. Second, we show how to construct an explicit solution at a higher level. In contrast with the lift that takes any solution as a black box, here we must directly understand and tackle the additional complicated structure imposed by the higher levels. Lastly, by relaxing the constraints, we are able to come up with a dual solution that shows completeness. We will now elaborate on each of these three new constructions of higher-order dual solutions.

Motivated by the proven strength of these new hierarchies (their completeness) and our extensive understanding of the first level of the hierarchy (i.e., Delsarte's original LPs), a natural question is how to *lift* a dual solution from level 1 to an arbitrary level ℓ, i.e., how to explicitly construct a level ℓ dual solution from a level 1 dual solution while (appropriately) retaining its objective value. A lift is one way to identify an explicit solution to level ℓ of the hierarchy whose value matches the Delsarte LP. Therefore, there may be potential to perturb the lifted solution in a direction which improves the objective value. Besides improving our understanding of how dual solutions are related to each other across multiple levels of the hierarchy, the additional structure of the dual at higher levels has the potential of leading to improvements in the objective value (in case the original Delsarte LPs suffer from integrality gap). We prove a general lifting result from a level k dual solution to level ℓ assuming that k divides ℓ. More precisely, our first structural result is given below.

Theorem 1.1 (Lifting Dual Solutions (Informal version of Theorem 4.9))**.** *Given an arbitrary dual feasible solution of level k, we can* explicitly *construct a new dual feasible solution of level $\ell \geqslant k$ provided k divides ℓ (this can be done over any finite field $\mathbb{F}_q$). Furthermore, this new dual solution has (appropriately) the same objective value of the given starting solution.*

Remark 1.2. *Unlike more structured convex programming hierarchies such as the Sum-of-Squares SDP hierarchy or Sherali-Adams LP hierarchy, establishing a lift for the higher-order Delsarte dual LPs is not trivial. We also stress that the value of the above theorem lies in its* explicitness*; "monotonicity" of the objective value was already established [CJJ22] (using the primal formulation), and this is not the point of the preceding theorem.*

Another natural question is whether we can construct dual feasible solutions for higher levels of these new hierarchies from scratch. As noted above, there are now a wealth of perspectives and techniques to construct dual feasible solutions to level 1 (the original Delsarte LPs). For instance, the original MRRW proof relies on properties of the Krawtchouk polynomials, which form a family of orthogonal polynomials, whereas some more recent proofs use spectral graph theory and Fourier analysis. Curiously, these various analyses are largely different perspectives or small variations of a single construction. Nonetheless, having multiple perspectives can be very helpful, and they can serve as (seemingly) different starting points for analyzing the hierarchies.

Although these hierarchies are structurally similar to the original LPs (coinciding at level 1), there are challenges to be addressed. First, the hierarchy at level $\ell \geqslant 2$ inherently relies on multivariate versions of Krawtchouk polynomials, as opposed to the univariate version of level 1. The asymptotic behavior of the first root of univariate Krawtchouk polynomials plays a crucial role in the original analysis, while establishing an analogous property in the multivariate case is less clear. Moreover, while level 1 is the same regardless of whether a code is linear or not (only the meaning of the variables changes), higher levels of these hierarchies have new constraints associated with linearity which pose new challenges.

Our second structural and main result is an explicit construction of dual feasible solutions to constant levels of the hierarchy for the important class of balanced linear codes[1], giving the first theoretical analysis of a convex programming hierarchy containing Delsarte's original LP. The main contribution here is to make sense of the higher-order structure of the hierarchy, suitably generalizing spectral-based techniques for the Delsarte LP. Obtaining such suitable generalization was met with substantial challenges (see Section 3) as it may be expected in analyzing *any* convex programming hierarchy strengthening Delsarte's LP since progress in this area has stalled in 1970s. The objective value of our constructed solutions approximately matches the state-of-the-art MRRW bound up to lower-order terms in ε. Our main result is stated below.

Theorem 1.3 (Higher-order Dual Solution (Informal version of Corollary 6.11 of Theorem 6.7))**.** *For every constant level $\ell \in \mathbb{N}_+$, there is an explicit construction of dual feasible solutions at level ℓ for binary ε-balanced linear codes with rate upper bound $R_2^\ell(\delta)$, with $\delta = (1-\varepsilon)/2$, satisfying*

$$R_2^\ell(\delta) = (1 + o_\varepsilon(1)) \cdot R_2^{\mathrm{MRRW}}(\delta),$$

where $R_2^{\mathrm{MRRW}}(\delta)$ is the rate upper bound of the first LP bound of [MRRW77].

The proof of the above theorem establishes a footprint of how to construct higher-order dual solutions, breaking the ice on the daunting complexity of higher-order convex programs. It may serve as a technical foundation for further quantitative improvements.

We now give some additional context before describing our third structural result. A feasible solution of the dual can be seen as a certificate establishing a universal upper bound on the size of codes. Ideally, the better we understand the structure and nature of these dual certificates, the better positioned we may be for designing new ones. The higher-order Delsarte hierarchies are known to converge to the true value of a linear code; however, the known proofs [CJJ22, CJJ23] are entirely based on the primal version of these hierarchies. It is then natural to ask if we can use the dual hierarchies to prove completeness. Our third result is a novel completeness proof of these hierarchies which uses their dual formulations.

Theorem 1.4 (Completeness from the Dual (Informal version of Theorem 5.1))**.** *The dual higher-order Delsarte LPs obtain the true value of a linear code for any level $\ell \geqslant n$ and over any finite field $\mathbb{F}_q$.*

Remark 1.5. *Unlike other more structured convex programming hierarchies, such as the Sum-of-Squares SDP hierarchy or Sherali-Adams LP hierarchy, (exact) completeness for the higher-order Delsarte's LP is not immediate [CJJ22, CJJ23].*

A better understanding of completeness from the dual may also help understand the power of natural LP hierarchies for lattice packings, extending the celebrated Cohn and Elkies LP for sphere

[1] Recall that, for $\varepsilon \in (0,1)$, an ε-balanced linear code is a code in which every non-zero codeword has Hamming weight in $[(1-\varepsilon)n/2, (1+\varepsilon)n/2]$.

packing [CE03, Via17, CKM$^+$17]. Recall that the Cohn and Elkies LP can be seen as a close analog of Delsarte's *dual* LP designed for sphere packing.

1.2 Organization

First, we recall the higher-order Delsarte LP hierarchies of [CJJ22, LL23b] in Section 2. We provide several different formulations of the hierarchies which will be used to establish our results (other equivalent formulations that will not be used in the present work are included in Appendix A for the curious reader). In Section 3, we give the main technical intuition of the proofs. We formally prove the lifting in Section 4. The completeness from dual is presented in Section 5. The spectral-based construction of higher-order dual feasible solutions is given in Section 6. We end with some concluding remarks in Section 7.

The reader should refer to Appendix B for notation as needed.

2 A Brief Introduction to the Hierarchies

Both hierarchies of [CJJ22, LL23b] can be used to upper bound sizes of linear codes in an arbitrary set of "valid" linear codes $\mathrm{Valid}_n \subseteq L_{\mathbb{F}_q}(\mathbb{F}_q^n)$. In the prototypical cases, Valid_n is the set of all linear codes of distance at least d, or the set of all ε-balanced codes. Once Valid_n is fixed, at level $\ell \in \mathbb{N}_+$ the hierarchies make use of the set

$$\mathrm{Valid}_{n,\ell} \stackrel{\mathrm{def}}{=} \{X \in \mathbb{F}_q^{\ell\times n} \mid \mathrm{span}(\{X_1,\ldots,X_\ell\}) \in \mathrm{Valid}_n\}.$$

The easiest way of stating the hierarchy of [CJJ22] at level ℓ is as the Lovász ϑ' of the graph $G_{n,\ell}$ over the vertex set $\mathbb{F}_q^{\ell\times n}$ in which $X, Y \in \mathbb{F}_q^{\ell\times n}$ are adjacent exactly when $X - Y \notin \mathrm{Valid}_{n,\ell}$. If $C \in \mathrm{Valid}_n$, then the set $\{X \in \mathbb{F}_q^{\ell\times n} \mid X_1, \ldots, X_\ell \in C\}$ is an independent set in $G_{n,\ell}$ of size exactly $|C|^\ell$, which is upper bounded by $\vartheta'(G_{n,\ell})$, giving us the first formulation of the hierarchy of (34) (which is deferred to Appendix A.1 as it will not be used in the present paper).

It turns out that the SDP arising in the Lovász ϑ' function can be explicitly diagonalized, leading to a linear program. By noting that there is a natural "global translation" action of $\mathbb{F}_q^n$ on the space $\mathbb{F}_q^{\ell\times n}$ given by

$$(z\cdot X)_{jk} \stackrel{\mathrm{def}}{=} X_{jk} + z_k \qquad (X \in \mathbb{F}_q^{\ell\times n}, z \in \mathbb{F}_q^n, j \in [\ell], k \in [n]),$$

and that the program (34) of $\vartheta'(G_{n,\ell})$ is $\mathbb{F}_q^n$-symmetric, every feasible solution can be symmetrized under this action without violating its feasibility or changing its value. Furthermore, $\mathbb{F}_q^n$-symmetric solutions are simultaneously diagonalizable and the positive semidefinite constraint is then encoded by the Fourier transform (see Appendix A.2 for more details) given by

$$\widehat{f}(X) \stackrel{\mathrm{def}}{=} \langle f, \chi_X\rangle = \frac{1}{q^{n\ell}} \sum_{X\in\mathbb{F}_q^{\ell\times n}} f(X)\overline{\chi_Z(X)} \qquad (f \in \mathbb{C}^{\mathbb{F}_q^{\ell\times n}}, X \in \mathbb{F}_q^{\ell\times n}),$$

$$\chi_Z(X) \stackrel{\mathrm{def}}{=} \exp\left(\sum_{j\in[\ell]}\sum_{k\in[n]} \frac{2\pi i X_{jk} Z_{jk}}{q}\right) \qquad (X \in \mathbb{F}_q^{\ell\times n}).$$

This yields the linear program (1) below, whose dual is (2) and that first appeared in [CJJ22]. A linear code $C \in \mathrm{Valid}_n$ yields a natural solution f_C of (1) given by $f_C(X) \overset{\text{def}}{=} \mathbb{1}[X_1, \ldots, X_\ell \in C]$, whose value is $|C|^\ell$. Note that when q is a power of 2, due to $X = -X$, the symmetry constraints in the primal are automatically enforced and we can therefore remove β from the dual.

$$\boxed{\begin{array}{llll} \text{Variables:} & f\colon \mathbb{F}_q^{\ell\times n} \to \mathbb{R} & & \\ \max & \displaystyle\sum_{X\in\mathbb{F}_q^{\ell\times n}} f(X) & & \\ \text{s.t.} & f(0) = 1 & & \text{(Normalization)} \\ & f(X) = 0 & \forall X \in \mathbb{F}_q^{\ell\times n} \setminus \mathrm{Valid}_{n,\ell} & \text{(Validity)} \\ & \widehat{f}(X) \geqslant 0 & \forall X \in \mathbb{F}_q^{\ell\times n} & \text{(Fourier)} \\ & f(X) \geqslant 0 & \forall X \in \mathbb{F}_q^{\ell\times n} & \text{(Non-negativity)} \\ & f(X) = f(-X) & \forall X \in \mathbb{F}_q^{\ell\times n} & \text{(Symmetry)} \end{array}} \tag{1}$$

$$\boxed{\begin{array}{llll} \text{Variables:} & g\colon \mathbb{F}_q^{\ell\times n} \to \mathbb{R}, \beta\colon \mathbb{F}_q^{\ell\times n} \to \mathbb{R} & & \\ \min & g(0) & & \\ \text{s.t.} & \widehat{g}(0) = 1 & & \text{(Normalization)} \\ & g(X) + \beta(X) - \beta(-X) \leqslant 0 & \forall X \in \mathrm{Valid}_{n,\ell} \setminus \{0\} & \text{(Validity)} \\ & \widehat{g}(X) \geqslant 0 & \forall X \in \mathbb{F}_q^{\ell\times n} & \text{(Non-negativity)} \end{array}} \tag{2}$$

Next, one observes that there is a natural "label permutation" action of S_n on $\mathbb{F}_q^{\ell\times n}$ given by

$$(\sigma \cdot X)_{ij} \overset{\text{def}}{=} X_{i\sigma(j)} \qquad (X \in \mathbb{F}_q^{\ell\times n}, \sigma \in S_n, i \in [\ell], j \in [n]).$$

It is easy to see that if Valid_n is S_n-symmetric under the natural action of S_n on $\mathbb{F}_q^n$, then so are $\mathrm{Valid}_{n,\ell}$ and (1) under the S_n-action above. This allows us to further symmetrize the program to obtain the formulation in (36) in which the Fourier transform is encoded using multivariate Krawtchouk polynomials (see Appendix A.3).

Finally, we introduce the Partial Fourier Hierarchy of [LL23b]. This hierarchy follows from the observation that the natural solutions $f_C(X) \overset{\text{def}}{=} \mathbb{1}[X_1, \ldots, X_\ell \in C]$ to (1) not only have non-negative Fourier transforms, but in fact have non-negative "partial Fourier transforms" defined as follows.

First, we note that $\mathrm{GL}_\ell(\mathbb{F}_q)$ also acts on $\mathbb{F}_q^{\ell\times n}$ by left-multiplication, which in turn induces a right-action of $\mathrm{GL}_\ell(\mathbb{F}_q)$ on the set of functions $\mathbb{F}_q^{\ell\times n} \to \mathbb{C}$ given by $(f \cdot M)(X) \overset{\text{def}}{=} f(M \cdot X)$. Then for $X, Y \in \mathbb{F}_q^{\ell\times n}$, $k \in \{0, 1, \ldots, n\}$ and $M \in \mathrm{GL}_\ell(\mathbb{F}_q)$, we let

$$\chi_Y^{(k)}(X) \overset{\text{def}}{=} q^{(\ell-k)n} \cdot \left(\prod_{j=1}^{k} \chi_{Y_j}(X_j)\right) \cdot \left(\prod_{j=k+1}^{n} \mathbb{1}_{Y_j}(X_j)\right), \qquad \chi_Y^{k,M}(X) \overset{\text{def}}{=} \chi_{M^{-1}\cdot Y}^{(k)}(M^{-1} \cdot X),$$

where $\chi_y(x) \overset{\text{def}}{=} \exp(\sum_{j\in[n]} 2\pi i y_j x_j / q)$ is the usual character and we let

$$\mathcal{F}_k(f)(X) \overset{\text{def}}{=} \langle f, \chi_X^{(k)} \rangle = \frac{1}{q^{\ell n}} \cdot \sum_{Z\in\mathbb{F}_q^{\ell\times n}} f(Z) \cdot \overline{\chi}_X^{(k)}(Z), \qquad \mathcal{F}_{k,M}(f)(X) \overset{\text{def}}{=} \langle f, \chi_X^{k,M} \rangle,$$

for every $f\colon \mathbb{F}_q^{\ell\times n}\to\mathbb{C}$. A straightforward calculation then yields

$$\mathcal{F}_{k,M}(f)=\mathcal{F}_k(f\cdot M)\cdot M^{-1}, \qquad\qquad \mathcal{F}_{k,M}^{-1}(f)=q^{kn}\cdot\mathcal{F}_{k,M}(f)\cdot R_k, \tag{3}$$

where R_k is the diagonal matrix whose diagonal consists of k entries -1 followed by $\ell-k$ entries 1.

Noting that for every $C\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ the function $f_C(X)\overset{\text{def}}{=}\mathbb{1}[X_1,\dots,X_\ell\in C]$ satisfies $\mathcal{F}_{k,M}(f_C)\geqslant 0$ ($k\in[\ell]$, $M\in\mathrm{GL}_\ell(\mathbb{F}_q)$), it follows that we can add further constraints to (1) to obtain a stronger hierarchy,[2] called the partial Fourier hierarchy [LL23b], formulated in (4) and whose rather technical dual (7) is deferred to Section 4. We will show in Lemma 4.2 that the dual of (4) is further equivalent to the simpler (5) below.

$$\boxed{\begin{array}{llll}
\text{Variables: } f\colon \mathbb{F}_q^{\ell\times n}\to\mathbb{R} & & & \\
\quad\max & \displaystyle\sum_{X\in\mathbb{F}_q^{\ell\times n}} f(X) & & \\
\quad\text{s.t.} & f(0)=1 & & \text{(Normalization)}\\
 & f(X)=0 & \forall X\in\mathbb{F}_q^{\ell\times n}\setminus\mathrm{Valid}_{n,\ell} & \text{(Validity)}\\
 & \mathcal{F}_{k,M}(f)(X)\geqslant 0 & \forall X\in\mathbb{F}_q^{\ell\times n},\forall k\in[\ell],\forall M\in\mathrm{GL}_\ell(\mathbb{F}_q) & \text{(Partial Fourier)}\\
 & f(X)\geqslant 0 & \forall X\in\mathbb{F}_q^{\ell\times n} & \text{(Non-negativity)}\\
 & f(X)=f(-X) & \forall X\in\mathbb{F}_q^{\ell\times n} & \text{(Symmetry)}
\end{array}} \tag{4}$$

$$\boxed{\begin{array}{llll}
\text{Variables: } g_k\colon \mathbb{F}_q^{\ell\times n}\to\mathbb{R}\ (k\in[\ell]) & & & \\
\quad\min & \displaystyle 1+\sum_{k\in[\ell]} g_k(0) & & \\
\quad\text{s.t.} & \displaystyle 1+\frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|}\cdot\sum_{\substack{k\in[\ell]\\ M\in\mathrm{GL}_\ell(\mathbb{F}_q)}}(g_k\cdot M)(X)\leqslant 0 & \forall X\in\mathrm{Valid}_{n,\ell}\setminus\{0\} & \text{(Validity)}\\
 & \mathcal{F}_k(g_k)\geqslant 0 & \forall k\in[\ell] & \text{(Partial Fourier)}
\end{array}} \tag{5}$$

3 Technical Overview of the Proofs

The purpose of this section is to highlight the main ideas of the proofs and provide intuition, in preparation for the full results. For simplicity, we restrict ourselves here to $q=2$.

3.1 Lifting Dual Solutions

A lift transforms a level-k solution of value V into a level-ℓ solution, with objective value $V^{\ell/k}$. The scaling is correct, since solutions in the hierarchy's ℓ-th level provide an upper-bound on $|C|^\ell$ for $C\in\mathrm{Valid}_n$. In our approach we construct functions $f^{(1)},f^{(2)},\dots,f^{(\ell/k)}$ that satisfy increasingly more constraints, and terminate with a feasible solution $f^{(\ell/k)}$.

[2] In fact, [LL23b] only includes partial Fouriers with $M=I$, but explicitly requires solutions to be $\mathrm{GL}_\ell(\mathbb{F}_q)$-symmetric; here we opt for this formulation which can be shown to be equivalent straightforwardly.

Here we illustrate our method with the LP (2) over $\mathbb{F}_2$. In Section 4, the lifts are developed in full for the stronger LP (5) over general finite fields, $\mathbb{F}_q$.

We start with a lift from level 1. Let $h' \colon \mathbb{F}_2^n \to \mathbb{R}$ be a feasible solution for level 1 of the dual hierarchy (2). It will be more convenient to work with $h \overset{\text{def}}{=} h' - 1$. Observe that

$$\widehat{h} \geqslant 0, \qquad \widehat{h}(0) = 0, \qquad \forall x \in \mathrm{Valid}_{n,1} \setminus \{0\}, h(x) \leqslant -1,$$

To lift h to level ℓ we start by defining

$$f^{(1)}(X) \overset{\text{def}}{=} h(X_1) \qquad \forall X = (X_1, \ldots, X_\ell) \in \mathbb{F}_2^{\ell \times n}.$$

Namely, we ignore all of the rows of X except for the first.

The Fourier transform of $f^{(1)}$ is non-negative, since $\widehat{h} \geqslant 0$. Also, $\widehat{f}^{(1)}(0) = 0$. These two properties persist throughout the process, for $f^{(2)}, f^{(3)}, \ldots$ etc.

The validity constraints are only satisfied if $X_1 \in \mathrm{Valid}_{n,1} \setminus \{0\}$: otherwise, $f^{(1)}(X) = h(0)$, which not only is positive but in fact exponentially large. To handle the case $X \in \mathrm{Valid}_{n,\ell}$ with $X_1 = 0$, we define

$$f^{(2)}(X) \overset{\text{def}}{=} f^{(1)}(X) + (1 + h(0)) \cdot h(X_2) \cdot \mathbb{1}[X_1 = 0]$$

Observe that $f^{(2)}$ only differs from $f^{(1)}$ when $X_1 = 0$. The validity constraints now hold if $(X_1, X_2) \in \mathrm{Valid}_{n,2}$, but not when $X_1 = X_2 = 0$.

We continue by defining, for $t = 3, \ldots, \ell$,

$$f^{(t)}(X) \overset{\text{def}}{=} f^{(t-1)}(X) + (1 + h(0))^{t-1} \cdot h(X_t) \cdot \mathbb{1}[X_{1,\ldots,t-1} = 0]$$

It is not hard to verify that $f^{(t)}$ satisfies[3]

$$\begin{aligned} &\widehat{f}^{(t)} \geqslant 0, && \widehat{f}^{(t)}(0) = 0, \\ &f^{(t)}(X) \leqslant -1 && \forall X \in \mathbb{F}_q^{\ell \times n} \text{ with } X_{1,\ldots,t} \in \mathrm{Valid}_{n,t} \setminus \{0\} \\ &f^{(t)}(X) = (1 + h(0))^t - 1 && \forall X \in \mathbb{F}_q^{\ell \times n} \text{ with } X_{1,\ldots,t} = 0. \end{aligned}$$

Thus, the function $f \overset{\text{def}}{=} f^{(\ell)} + 1$ is a feasible solution and $f(0) = (1 + h(0))^\ell = h'(0)^\ell$. This concludes the lift from level 1 to level ℓ in the LP (2).

The lift from level k to level ℓ proceeds similarly, except that we advance in chunks of k rows per step. Suppose we have a level-k feasible solution to the hierarchy (2), $h' \colon \mathbb{F}_2^{k \times n} \to \mathbb{R}$, and let $h \overset{\text{def}}{=} h' - 1$. We define

$$\begin{aligned} &f^{(0)} \overset{\text{def}}{=} 0 \\ &f^{(t)} \overset{\text{def}}{=} f^{(t-1)} + (1 + h(0))^{t-1} \cdot h(X_{k\cdot(t-1)+1,\ldots,k\cdot t}) \cdot \mathbb{1}[X_{1,\ldots,k\cdot(t-1)}] \qquad (t \in [\ell/k]). \end{aligned}$$

Then, similar arguments show that $f \overset{\text{def}}{=} f^{(\ell/k)} + 1$ is feasible for level ℓ, and its value is $f(0) = h'(0)^{\ell/k}$.

Our strategy remains unchanged as we move to the stronger LP (5). However, the symmetry operation in the validity constraints calls for a slight change in the argument. Rather than arguing

[3] In fact, there holds, moreover: $f^{(t)}(X) \leqslant -1$ for every X such that $X_{1,\ldots,t} \neq 0$ and $\{X_1, \ldots, X_t\} \subset \mathrm{Valid}_{n,1}$.

in terms of the number of zero rows in X, we now account by X's rank. Let $h_1, \ldots, h_k$ be a feasible solution to level k, that is

$$\begin{aligned} \mathcal{F}_i(h_i) &\geqslant 0 && \forall i \in [k], \\ 1 + \sum_{i=1}^{k} \mathbb{E}_{\boldsymbol{M} \sim U(\mathrm{GL}_\ell(\mathbb{F}_q))}[h_i(M \cdot X)] &\leqslant 0 && \forall X \in \mathrm{Valid}_{n,k} \setminus \{0\}, \end{aligned}$$

where $U(\mathrm{GL}_\ell(\mathbb{F}_q))$ is the uniform distribution on $\mathrm{GL}_\ell(\mathbb{F}_q)$ and the value of $(h_1, \ldots, h_k)$ is $V_h \stackrel{\text{def}}{=} 1 + \sum_{i\in[k]} h_i(0)$.

We would like to put the information of this level-k solution in the top k levels of a level-ℓ solution g, that is, we would like to put the information $h_1, \ldots, h_k$ into $g_{\ell-k+1}, \ldots, g_\ell$, respectively; we will then set $g_1 \stackrel{\text{def}}{=} \cdots \stackrel{\text{def}}{=} g_{\ell-k} \stackrel{\text{def}}{=} 0$. Furthermore, this needs to be organized so that the constraints $\mathcal{F}_i(g_i) \geqslant 0$ follow directly from the constraints $\mathcal{F}_i(h_i) \geqslant 0$. To do so, the solution is slightly permuted around when compared to the previous cases.

For each $i \in [k]$, we define a sequence of functions $f_i^{(1)}, f_i^{(2)}, \ldots, f_i^{(\ell/k)}$ as follows:

$$f_i^{(0)} \stackrel{\text{def}}{=} 0, \qquad f_i^{(t)} \stackrel{\text{def}}{=} f_i^{(t-1)} + V_h^{t-1} \cdot h_i(X_{\ell-k+1,\ldots,\ell}) \cdot \mathbb{1}[X_{1,\ldots,kt} = 0] \qquad (t \in [\ell/k]).$$

We will then argue that for every $t \in [\ell/k]$, we have

$$\begin{aligned} \mathcal{F}_{\ell-k+i}(f_i^{(t)}) &\geqslant 0 && \forall i \in [k], \\ 1 + \sum_{i=1}^{k} \mathbb{E}_{\boldsymbol{M} \sim U(\mathrm{GL}_\ell(\mathbb{F}_q))}[f_i^{(t)}(M \cdot X)] &\leqslant 0 && \forall X \in \mathrm{Valid}_{n,\ell} \setminus \{0\} \text{ with } \mathrm{rk}(X) \geqslant \ell - t \cdot k. \end{aligned}$$

Consequently, letting $g_i \stackrel{\text{def}}{=} 0$ for eveery $i \in [\ell - k]$ and $g_i \stackrel{\text{def}}{=} f_{i-\ell+k}^{(\ell/k)}$ for $\ell - k + 1 \leqslant i \leqslant \ell$, we obtain a feasible solution whose value is $V_h^{\ell/k}$.

3.2 Spectral-based Construction of Dual Solutions

We describe now how we use spectral techniques to construct dual solutions for the hierarchy. We start with an abstract description of the idea, then move to its realization in Delsarte's case, and finally to the way that we implement it in higher levels of the hierarchy. Throughout this section, we refer only to the LP hierarchy (2) over $\mathbb{F}_2$, of which level 1 is Delsarte's LP.

We begin with the abstract construction, which is mostly inspired by [NS05], and presented with more detail in [LL22, Sam23a]. Although this abstract construction is relatively intuitive, fully implementing it for the higher-order hierarchy is far from trivial as the reader will see in this paper. One can form a feasible $f\colon \mathbb{F}_2^{\ell\times n} \to \mathbb{R}$ by defining

$$f(X) \stackrel{\text{def}}{=} \frac{\phi(X) \cdot \Gamma^2(X)}{\widehat{\phi \cdot \Gamma^2}(0)},$$

where $\phi, \Gamma\colon \mathbb{F}_2^{\ell\times n} \to \mathbb{R}$ are not identically zero, and satisfy

$$\forall X \in \mathrm{Valid}_{n,\ell} \setminus \{0\}, \phi(X) \leqslant 0, \qquad \widehat{\Gamma} \geqslant 0, \qquad 2^{n\ell}\widehat{\phi} * \widehat{\Gamma} \geqslant \widehat{\Gamma}.$$

The sign of f is governed by ϕ, hence it fulfills the validity constraints. The Fourier constraints are met, because, by the convolution theorem, $\widehat{f}$ is up to positive constants equal to $\widehat{\phi} * \widehat{\Gamma} * \widehat{\Gamma} \geqslant 2^{-n\ell}\widehat{\Gamma} * \widehat{\Gamma} \geqslant 0$. An upper bound on the objective function is derived using Cauchy-Schwarz as follows

$$f(0) \leqslant 2^{n\ell}\phi(0) \cdot \frac{\Gamma^2(0)}{(\widehat{\Gamma} * \widehat{\Gamma})(0)} = 2^{n\ell}\phi(0) \cdot \frac{\|\widehat{\Gamma}\|_1^2}{\|\widehat{\Gamma}\|_2^2} \overset{\text{C.S}}{\leqslant} \phi(0) \cdot |\mathrm{supp}(\widehat{\Gamma})|.$$

One usually fixes ϕ as a low-degree polynomial, and seeks a feasible Γ so that $|\mathrm{supp}(\widehat{\Gamma})|$ is minimal.

The operator "$2^{n\ell}\widehat{\phi} * -$" of convolution by $\widehat{\phi}$ (up to renormalization) can be represented by a matrix which we denote $M_\phi \in \mathbb{R}^{\mathbb{F}_2^{\ell\times n}\times\mathbb{F}_2^{\ell\times n}}$, that is, we have

$$M_\phi h = 2^{n\ell}\widehat{\phi} * h, \quad (h\colon \mathbb{F}_2^{\ell\times n} \to \mathbb{R}).$$

Thus, finding Γ becomes a spectral problem.

When $\ell = 1$ and working with distance-d codes, ϕ can be as simple as the linear function $\phi_{\mathrm{MRRW}}(x) = 2(d - |x|)$, which is usually the case. The corresponding matrix is $M_{\phi_{\mathrm{MRRW}}} = A - (n-2d)I$, where A is the adjacency matrix of the Hamming graph, $A(x,y) = \mathbb{1}[|x-y| = 1]$. The problem of finding an appropriate Γ is well explored. It can be done through different techniques, e.g., specific properties of Krawtchouk Polynomials [MRRW77], Perron-Frobenius Theorem [BN06], or by taking advantage of the fact that the matrix A is highly symmetric [NS05].

As ℓ grows, however, the set $\mathrm{Valid}_{n,\ell}$ becomes increasingly complicated and cannot be captured or closely approximated by a linear function. Constructing a satisfactory ϕ is a problem in itself, which was first addressed in [LL22]. Finding a complementary Γ was left by the authors of [LL22] as an open problem. The methods used to find Γ in Delsarte's case $\ell = 1$ are inapplicable here due to the high-dimensionality of the problem, and the complicated structure of the corresponding matrix M_ϕ.

In the current work we solve this open problem for a variation of the suggested polynomial ϕ, which is valid for ε-balanced linear codes. The polynomial, denoted Φ_m, is defined in (20) and its necessary properties are established in Lemma 6.5. We find an appropriate Γ for Φ_m which leads to a feasible solution whose value is equivalent to MRRW, up to lower order terms.

Our strategy is as follows. First, we show (Lemma 6.6) that the matrix M_m, which corresponds to the operator "$2^{n\ell}\widehat{\Phi}_m * -$", is a sum of terms of the form

$$\left(\prod_{u\in U} \sum_{\substack{v\in\mathbb{F}_2^\ell \\ \langle u,v\rangle=1}} A_v^m\right) \cdot \left(\frac{1}{k} \cdot \sum_{\substack{v\in\mathbb{F}_2^\ell \\ \langle i,v\rangle=1}} A_v^m - \frac{2^{\ell-1}(\varepsilon n)^m}{2^\ell - k}\right)$$

with non-negative coefficients. Here,

- A_v, for every $v \in \mathbb{F}_2^\ell \setminus \{0\}$, is the adjacency matrix of a graph over the vertex set $\mathbb{F}_2^{\ell\times n}$, where X, Y are adjacent if X is obtained from Y by adding v to one of its columns.
- $m \in \mathbb{N}$ is even,
- $1 \leqslant k \leqslant 2^\ell - 1$,
- $i \in \mathbb{F}_2^\ell \setminus \{0\}$,

- $U \subseteq \mathbb{F}_2^\ell \setminus \{0\}$.

Noting that for every $i \in \mathbb{F}_2^\ell \setminus \{0\}$, there exists at least one $v \in \mathbb{F}_2^\ell$ with $\langle i, v\rangle = 1$ and $|v| = 1$, a sufficient condition for $M_m \cdot \widehat{\Gamma} \geqslant \widehat{\Gamma}$ is that

$$A_v^m \widehat{\Gamma} \geqslant (2^{2\ell-1}\varepsilon^m n^m + 1)\widehat{\Gamma} \tag{6}$$

for every $v \in \mathbb{F}_2^\ell$ with $|v| = 1$.

Solving for each A_v individually is analogous to the $\ell = 1$ case. It is less clear, however, how the above methods can be employed to solve jointly for all A_v. To this end we use the combinatorial argument of [LL23a], as follows. Let $F \subseteq \mathbb{F}_2^{\ell \times n}$ and let $\widehat{\Gamma}(X) = \mathbb{1}[X \in F]$. Consider the inequalities in (6): if $X \in \mathbb{F}_2^{\ell\times n} \setminus F$, the right-hand side is zero, while the left-hand side is non-negative. Otherwise, $X \in F$ and the left-hand side is the number of walks on the graph of A_v, of length m, that start at X and end in F.

It remains to choose a set F with minimal size and at least $2^{2\ell-1}\varepsilon^m n^m + 1$ many returning walks. The symmetry of the problem suggests to seek F among the *configuration* sets, i.e., the orbits of $\mathbb{F}_2^{\ell\times n}$ with respect to the S_n-action. In Lemmas 6.3 and 6.4, we count the returning walks for configurations. In Section 6.3, we choose configurations that lead to the desired result.

3.3 Completeness via Subspace Symmetric Dual LPs

We now provide an overview of some ingredients and ideas in the completeness proof from Section 5. As mentioned above, this new proof will take place in the dual formulation of these hierarchies, as opposed to the proof of [CJJ23], which takes place entirely in their primal formulation. Consequently, this new proof will be useful in shedding new light on the structure of the dual.

Recall that our goal is to prove that the hierarchy (2) is *exactly complete* at level n: its optimum is the maximum $|C|^\ell$ for $C \in \mathrm{Valid}_n$, for every $\ell \geqslant n$. Note that this will imply the same for the stronger partial Fourier hierarchy of [LL23b] (see (4), (5) and (7)). Our starting point will be the subspace symmetric formulation of these hierarchies from [CJJ23]. We recall this formulation later, in (12), and provide its dual in (13), but we will not need their precise details in this high-level overview.

The proof proceeds as follows. If the hierarchy is indeed complete at level ℓ, then there exists a dual solution whose value is $q^{k\ell}$, where $k \overset{\text{def}}{=} \max\{\dim_{\mathbb{F}_q}(C) \mid C \in \mathrm{Valid}_n\}$. However, constructing such a solution directly seems extremely hard. Instead, we consider a weaker hierarchy, by replacing the set Valid_n, which depends on the code's distance, with the set $\mathrm{Valid}_n^{\dim \leqslant k}$, which includes all linear codes of dimension at most k. We observe that

$$\mathrm{Valid}_n \subseteq \mathrm{Valid}_n^{\dim\leqslant k}, \qquad \max\{|C| \mid C \in \mathrm{Valid}_n\} = \max\{|C| \mid C \in \mathrm{Valid}_n^{\dim\leqslant k}\}$$

We then proceed to analyze this weaker hierarchy since it suffices to prove its completeness to deduce that the original hierarchy is also complete. A key observation is that to obtain the desired tight objective value $q^{k\ell}$ several LP variables are forced to be zero. This will simplify the structure of the dual, leading to a recurrence relating the value of the remaining variables.

4 Lifting Dual Solutions

In this section we show that dual solutions lift. That is, from a solution h at a level k of value V_h, we can construct a natural solution at any level ℓ divisible by k with value $V_h^{\ell/k}$. Let us point out that in terms of values, it was already known from [CJJ22, Corollary 6.6] that the value of the hierarchy (1) at level ℓ was at most the ℓ/kth power of its value at level k (provided k divides ℓ); the main contribution of this section is an explicit lift of dual solutions and the analogous result for the partial Fourier hierarchy (4), which does not immediately follow from the results of [CJJ22].

4.1 Further Symmetrization of the Dual

Our first order of business is to use the $\mathrm{GL}_\ell(\mathbb{F}_q)$-symmetry to simplify the dual program. We start by recalling that the standard dual of the partial Fourier hierarchy of (4) is (7) below.

$$\boxed{\begin{array}{ll}
\text{Variables: } & h_{k,M}\colon \mathbb{F}_q^{\ell\times n} \to \mathbb{R}\ (k \in [\ell], M \in \mathrm{GL}_\ell(\mathbb{F}_q), \beta\colon \mathbb{F}_q^{\ell\times n} \to \mathbb{R} \\
\min & 1 + \displaystyle\sum_{\substack{k\in[\ell] \\ M\in\mathrm{GL}_\ell(\mathbb{F}_q)}} \mathcal{F}_{k,M}(h_{k,M})(0) \\
\text{s.t.} & 1 + \displaystyle\sum_{\substack{k\in[\ell] \\ M\in\mathrm{GL}_\ell(\mathbb{F}_q)}} \mathcal{F}_{k,M}(h_{k,M})(X) + \beta(X) - \beta(-X) \leqslant 0 \quad \forall X \in \mathrm{Valid}_{n,\ell} \setminus \{0\} \quad \text{(Validity)} \\
 & h_{k,M}(X) \geqslant 0 \qquad \forall X \in \mathbb{F}_q^{\ell\times n}, \forall k \in [\ell], \forall M \in \mathrm{GL}_\ell(\mathbb{F}_q) \qquad \text{(Non-negativity)}
\end{array}} \tag{7}$$

Remark 4.1. *It will also be useful to think of hierarchy (2) as a special case of (7) above. For this, note that every solution of (2) yields a solution of (7) with the same value by setting $h_{\ell,I} \overset{\text{def}}{=} 2^{n\ell}(\widehat{g} - \mathbb{1}_0)$ and setting all other $h_{k,M}$ to zero. Conversely, if $((h_{k,M})_{k,M}, \beta)$ is a solution of (7) such that $h_{k,M} = 0$ whenever $(k,M) \neq (\ell, I)$, then we can obtain a solution of (2) of better or equal value by taking $g \overset{\text{def}}{=} (1 + \widehat{h}_{\ell,I})/(1 + 2^{n\ell} h_{\ell,I}(0))$. Thus, hierarchy (2) is equivalent to (7) with the extra constraints that $h_{k,M} = 0$ whenever $(k,M) \neq (\ell, I)$.*

We will now symmetrize (7) and pass to the Fourier basis, proving that it is equivalent to (5).

Lemma 4.2. *If $((h_{k,M})_{k,M}, \beta)$ is a solution of (7), then letting*

$$g_k \overset{\text{def}}{=} \sum_{M\in\mathrm{GL}_\ell(\mathbb{F}_q)} \mathcal{F}_{k,M}(h_{k,M}) \cdot M \qquad (k \in [\ell])$$

yields a solution of (5) with the same value.

Conversely, if $(g_k)_k$ is a solution of (5), then letting

$$\begin{aligned} h_{k,M} &\overset{\text{def}}{=} \frac{q^{kn}}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \mathcal{F}_{k,M}(g_k \cdot M) \qquad (k \in [\ell], M \in \mathrm{GL}_\ell(\mathbb{F}_q)), \\ \beta &\overset{\text{def}}{=} 0, \end{aligned}$$

yields a solution of (7) with the same value.

Proof. For the first direction, note that for $X \in \mathrm{Valid}_{n,\ell}$ (zero or not), we have

$$\begin{aligned}
&1 + \frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \sum_{\substack{k\in[\ell] \\ M\in\mathrm{GL}_\ell(\mathbb{F}_q)}} (g_k \cdot M)(X) \\
&\quad = 1 + \frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \sum_{k\in[\ell]} \sum_{M,N\in\mathrm{GL}_\ell(\mathbb{F}_q)} (\mathcal{F}_{k,N}(h_{k,N}) \cdot (N \cdot M))(X) \\
&\quad = \frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \sum_{M\in\mathrm{GL}_\ell(\mathbb{F}_q)} \left(1 + \sum_{k\in[\ell]} \sum_{N\in\mathrm{GL}_\ell(\mathbb{F}_q)} \mathcal{F}_{k,N}(h_{k,N})(M \cdot X) + \beta(M \cdot X) - \beta(-M \cdot X) \right),
\end{aligned}$$

where the last equality follows by a change of variables and since the β contributions cancel out when we sum over M.

Since $\mathrm{Valid}_{n,\ell}$ is $\mathrm{GL}_\ell(\mathbb{F}_q)$-invariant, if $X \neq 0$, then the above is simply an average of the left-hand side of the validity constraints in (7), so it must be non-positive.

On the other hand, if $X = 0$, then the first expression in the above is the objective value of (5) and the last expression is the objective of (7) (as both the average over M goes away and the β contributions cancel out since $M \cdot 0 = 0$).

Finally, note that by (3), we have

$$\begin{aligned}
\mathcal{F}_k(g_k) &= \sum_{M\in\mathrm{GL}_\ell(\mathbb{F}_q)} \mathcal{F}_k(\mathcal{F}_{k,M}(h_{k,M}) \cdot M) \\
&= \sum_{M\in\mathrm{GL}_\ell(\mathbb{F}_q)} \mathcal{F}_{k,M}(\mathcal{F}_{k,M}(h_{k,M})) \cdot M \\
&= q^{-kn} \cdot \sum_{M\in\mathrm{GL}_\ell(\mathbb{F}_q)} h_{k,M} \cdot R_k^{-1} \cdot M.
\end{aligned}$$

Since $h_{k,M} \geqslant 0$ for every $M \in \mathrm{GL}_\ell(\mathbb{F}_q)$, we conclude that $\mathcal{F}_k(g_k) \geqslant 0$.

We now prove the converse. Note that for $X \in \mathrm{Valid}_{n,\ell}$ (zero or not), we have

$$\begin{aligned}
&1 + \sum_{\substack{k\in[\ell] \\ M\in\mathrm{GL}_\ell(\mathbb{F}_q)}} \mathcal{F}_{k,M}(h_{k,M})(X) + \beta(X) - \beta(-X) \\
&\quad = 1 + \sum_{\substack{k\in[\ell] \\ M\in\mathrm{GL}_\ell(\mathbb{F}_q)}} \frac{q^{kn}}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \mathcal{F}_{k,M}(\mathcal{F}_{k,M}(g_k \cdot M))(X) \\
&\quad = 1 + \frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \sum_{\substack{k\in[\ell] \\ M\in\mathrm{GL}_\ell(\mathbb{F}_q)}} (g_k \cdot M \cdot R_k^{-1})(X),
\end{aligned}$$

where the second equality follows from (3).

Since $\mathrm{Valid}_{n,\ell}$ is $\mathrm{GL}_\ell(\mathbb{F}_q)$-invariant, if $X \neq 0$, then the above is non-positive as it is the left-hand side of a validity constraint in (5).

On the other hand, if $X = 0$, then the first expression in the above is the objective value of (7) (as the β contributions cancel out) and the last expression is the objective value of (5) (as the average over M goes away in the latter since $M \cdot R_k^{-1} \cdot 0 = 0$).

Finally, note that (3) implies

$$h_{k,M} = \frac{q^{kn}}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \mathcal{F}_{k,M}(g_k \cdot M^{-1}) = \frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \mathcal{F}_k(g_k) \cdot M^{-1}.$$

Since $\mathcal{F}_k(g_k) \geqslant 0$, we conclude that $h_{k,M} \geqslant 0$. ■

Remark 4.3. *Recalling from Remark 4.1 that hierarchy (2) is equivalent to (7) with the extra constraints that $h_{k,M} = 0$ whenever $(k, M) \neq (\ell, I)$, an analogue of Lemma 4.2 shows that the dual above is equivalent to (5) with the extra constraints that $g_k = 0$ for every $k \in [\ell - 1]$.*

4.2 Basic Properties

We now prove some basic combinatorial properties about matrices over $\mathbb{F}_q$.

Lemma 4.4. *For a prime power q and $\ell \in \mathbb{N}$, the group*

$$\mathrm{GL}_\ell(\mathbb{F}_q) \stackrel{\mathrm{def}}{=} \{M \in \mathbb{F}_q^{\ell\times\ell} \mid \det(M) \neq 0\}$$

has size exactly

$$(q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot \ell!_q$$

Proof. By iteratively counting how many columns preserve linear independence, we get

$$|\mathrm{GL}_\ell(\mathbb{F}_q)| = \prod_{j=0}^{\ell-1}(q^\ell - q^j) = (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot \prod_{j=0}^{\ell-1}[\ell - j]_q = (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot \ell!_q. \qquad ■$$

Definition 4.5. *Let q be a prime power, let $s, t, \ell, n \in \mathbb{N}$ with $s \leqslant t \leqslant \ell \leqslant n$ and let $X \in \mathbb{F}_q^{\ell\times n}$. We define*

$$M_q^{s,t}(X) \stackrel{\mathrm{def}}{=} \{M \in \mathrm{GL}_\ell(\mathbb{F}_q) \mid (M \cdot X)_{1,\ldots,s} = 0 \wedge (M \cdot X)_{t+1,\ldots,\ell} = 0\}.$$

When $t = \ell$, we will use the shorthand notation $M_q^s(X) \stackrel{\mathrm{def}}{=} M_q^{s,\ell}(X)$.

Furthermore, we define the marginal action of $\mathrm{GL}_s(\mathbb{F}_q)$ on $\mathrm{GL}_\ell(\mathbb{F}_q)$ by

$$N \cdot M \stackrel{\mathrm{def}}{=} \begin{pmatrix} N & 0 \\ 0 & I \end{pmatrix} \cdot M \qquad (N \in \mathrm{GL}_s(\mathbb{F}_q), M \in \mathrm{GL}_\ell(\mathbb{F}_q))$$

(on the right-hand side, the identity matrix is of order $\ell - s$ and the product is the usual matrix product).

Lemma 4.6. *Let q be a prime power, let $s, t, \ell, n \in \mathbb{N}$ with $s \leqslant t \leqslant \ell \leqslant n$ and let $X \in \mathbb{F}_q^{\ell\times n}$. Then the following hold.*

i. The sets $M_q^{0,t}(X)$ and $M_q^{s,t}(X)$ are $\mathrm{GL}_s(\mathbb{F}_q)$-invariant.

ii. If $\boldsymbol{M}$ is picked uniformly at random in $M_q^{0,t}(X)$, then the distribution of $(\boldsymbol{M} \cdot X)_{1,\ldots,s}$ is $\mathrm{GL}_s(\mathbb{F}_q)$-invariant.

iii. For $z = s + \ell - t$ and $r \overset{\text{def}}{=} \operatorname{rk}(X)$, we have

$$|M_q^{s,t}(X)| = |M_q^z(X)| = (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot (\ell - z)_{r,q} \cdot (\ell - r)!_q.$$

Proof. Item (i) follows since for every $N \in \mathrm{GL}_s(\mathbb{F}_q)$ and every $M \in \mathrm{GL}_\ell(\mathbb{F}_q)$, we have

$$\left(\begin{pmatrix} N & 0 \\ 0 & I \end{pmatrix} \cdot M \cdot X\right)_{1,\ldots,s} = 0 \iff (M \cdot X)_{1,\ldots,s} = 0,$$
$$\left(\begin{pmatrix} N & 0 \\ 0 & I \end{pmatrix} \cdot M \cdot X\right)_{t+1,\ldots,\ell} = 0 \iff (M \cdot X)_{t+1,\ldots,\ell} = 0.$$

For Item (ii), note that the distribution of $\boldsymbol{M}$ is $\mathrm{GL}_s(\mathbb{F}_q)$-invariant. Thus, for every $N \in \mathrm{GL}_s(\mathbb{F}_q)$, we have

$$N \cdot (\boldsymbol{M} \cdot X)_{1,\ldots,s} = \left(\begin{pmatrix} N & 0 \\ 0 & I \end{pmatrix} \cdot \boldsymbol{M} \cdot X\right)_{1,\ldots,s} \sim (\boldsymbol{M} \cdot X)_{1,\ldots,s}.$$

It remains to prove Item (iii).

The fact that $|M_q^{s,t}(X)| = |M_q^z(X)|$ follows since there is a natural bijection between these sets obtained by permuting rows $s+1,\ldots,z$ with rows $t+1,\ldots,\ell$.

Let us then compute the size of $M_q^z(X)$. First note that for every $N \in \mathrm{GL}_\ell(\mathbb{F}_q)$, we have

$$M_q^z(N \cdot X) = \{M \cdot N^{-1} \mid M \in M_q^z(X)\},$$

so it suffices to show only the case when

$$X_1 = e_1, X_2 = e_2, \ldots, X_z = e_z, X_{z+1} = 0, X_{z+2} = 0, \ldots, X_\ell = 0,$$

where $e_i \in \mathbb{F}_q^n$ is the ith canonical basis vector.

By decomposing an element $M \in M_q^z(X)$ into blocks as

$$M = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

such that $A \in \mathbb{F}_q^{z \times r}$, $B \in \mathbb{F}_q^{z \times (n-r)}$, $C \in \mathbb{F}_q^{(\ell-z)\times r}$ and $D \in \mathbb{F}_q^{(\ell-z)\times(n-r)}$, we note that we must have $A = 0$, so we can count the elements of $M_q^z(X)$ by iteratively counting how many columns preserve linear independence to get

$$|M_q^z(X)| = \left(\prod_{j=0}^{r-1}(q^{\ell-z} - q^j)\right) \cdot \prod_{j=r}^{\ell-1}(q^\ell - q^j) = (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot (\ell - z)_{r,q} \cdot (\ell - r)!_q,$$

as desired. ∎

4.3 The Lifts

We now have all the ingredients to lift dual solutions. We start with a warm-up by lifting solutions from level 1 to level ℓ. The bold reader should feel free to skip directly to Theorem 4.9.

Proposition 4.7. *Let q be a prime power. If h is a solution of (5) with $\ell = 1$, then for every $\ell \in [n]$, letting*

$$g_1 \overset{\text{def}}{=} g_2 \overset{\text{def}}{=} \cdots \overset{\text{def}}{=} g_{\ell-1} \overset{\text{def}}{=} 0, \qquad g_\ell(X) \overset{\text{def}}{=} \sum_{t\in[\ell]} (1+h(0))^{\ell-t} \cdot h(X_1) \cdot \mathbb{1}[X_{t+1,\dots,\ell} = 0]$$

gives a solution of (5) whose objective value is the ℓth power of the objective value of h, i.e., we have

$$1 + \sum_{u\in[\ell]} g_u(0) = (1+h(0))^\ell.$$

Proof. Clearly $\mathcal{F}_u(g_u) = 0$ for every $u \in [\ell-1]$. Also, for every $X \in \mathbb{F}_q^{\ell\times n}$, we have

$$\mathcal{F}_\ell(g_\ell)(X) = \sum_{t\in[\ell]} (1+h(0))^{\ell-t} \cdot \widehat{h}(X_1) \cdot \mathbb{1}[X_{2,\dots,t} = 0] \cdot 2^{-n(\ell-t)},$$

which is non-negative as $\widehat{h} = \mathcal{F}_1(h) \geqslant 0$.

Let us now show the validity constraints. Let $X \in \mathrm{Valid}\setminus\{0\}$ and let $r \overset{\text{def}}{=} \mathrm{rk}(X)$. We need to show that

$$1 + \frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \sum_{u\in[\ell]} \sum_{M\in\mathrm{GL}_\ell(\mathbb{F}_q)} (g_u \cdot M)(X) \leqslant 0,$$

which is equivalent to

$$\sum_{t\in[\ell]} (1+h(0))^{\ell-t} \cdot \frac{1}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \cdot \sum_{M\in\mathrm{GL}_\ell(\mathbb{F}_q)} h((M\cdot X)_1) \cdot \mathbb{1}[(M\cdot X)_{t+1,\dots,\ell} = 0] \leqslant -1,$$

which in turn is equivalent to

$$\sum_{t\in[\ell]} (1+h(0))^{\ell-t} \cdot \mathbb{E}_{\boldsymbol{M}\sim U(\mathrm{GL}_\ell(\mathbb{F}_q))}[h((\boldsymbol{M}\cdot X)_1) \cdot \mathbb{1}[(\boldsymbol{M}\cdot X)_{t+1,\dots,\ell} = 0]] \leqslant -1, \tag{8}$$

where $U(\mathrm{GL}_\ell(\mathbb{F}_q))$ is the uniform distribution on $\mathrm{GL}_\ell(\mathbb{F}_q)$.

To prove the above, fix $t \in [\ell]$ and let us study the expression $h((\boldsymbol{M}\cdot X)_1) \cdot \mathbb{1}[(\boldsymbol{M}\cdot X)_{t+1,\dots,\ell} = 0]$.

First, recalling Definition 4.5, we partition $\mathrm{GL}_\ell(\mathbb{F}_q)$ into the sets

$$M_q^{1,t}(X), \qquad M_q^{0,t}(X) \setminus M_q^{1,t}(X), \qquad \mathrm{GL}_\ell(\mathbb{F}_q) \setminus M_q^{0,t}(X),$$

which by Lemmas 4.4 and 4.6 have sizes

$$\begin{gathered}(q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot (t-1)_{r,q} \cdot (\ell-r)!_q,\\ (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot ((t)_{r,q} - (t-1)_{r,q}) \cdot (\ell-r)!_q,\\ (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot ((\ell)_{r,q} - (t)_{r,q}) \cdot (\ell-r)!_q,\end{gathered} \tag{9}$$

respectively.

Note that $\mathbb{1}[(\boldsymbol{M} \cdot X)_{t+1,\ldots,\ell} = 0]$ only takes non-zero values when $\boldsymbol{M}$ is in one of the first two sets.

Clearly, if we condition on $\boldsymbol{M} \in M_q^{1,t}(X)$, then $(\boldsymbol{M} \cdot X)_1 = 0$.

On the other hand, by Items (i) and (ii) of Lemma 4.6, we know that the conditional distribution of $(\boldsymbol{M} \cdot X)_1$ given $\boldsymbol{M} \in M_q^{0,t}(X) \setminus M_q^{1,t}(X)$ is $\mathrm{GL}_1(\mathbb{F}_q)$-invariant. In particular, this implies that if $\boldsymbol{N} \sim U(\mathrm{GL}_1(\mathbb{F}_q))$ is independent from $\boldsymbol{M}$, then the conditional distributions of $(\boldsymbol{M} \cdot X)_1$ and $\boldsymbol{N} \cdot (\boldsymbol{M} \cdot X)_1$ given $\boldsymbol{M} \in M_q^{0,t}(X) \setminus M_q^{1,t}(X)$ are the same. Finally, since $X \in \mathrm{Valid} \setminus \{0\}$, we know that when we condition on $\boldsymbol{M} \in M_q^{0,t}(X) \setminus M_q^{1,t}(X)$, then $(\boldsymbol{M} \cdot X)_1$ is always an element of $\mathrm{Valid} \setminus \{0\}$. Thus we conclude that

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{M}}[h((\boldsymbol{M} \cdot X)_1) \cdot \mathbb{1}[(\boldsymbol{M} \cdot X)_{t+1,\ldots,\ell} = 0] \mid \boldsymbol{M} \in M_q^{1,t}(X)] &= h(0), \\
\mathbb{E}_{\boldsymbol{M}}[h((\boldsymbol{M} \cdot X)_1) \cdot \mathbb{1}[(\boldsymbol{M} \cdot X)_{t+1,\ldots,\ell} = 0] \mid \boldsymbol{M} \in M_q^{0,t}(X) \setminus M_q^{1,t}(X)]& \\
= \mathbb{E}_{\boldsymbol{M}}[\mathbb{E}_{\boldsymbol{N}}[h(\boldsymbol{N} \cdot (\boldsymbol{M} \cdot X)_1)] \mid \boldsymbol{M} \in M_q^{0,t}(X) \setminus M_q^{1,t}(X)] &\leqslant -1, \\
\mathbb{E}_{\boldsymbol{M}}[h((\boldsymbol{M} \cdot X)_1) \cdot \mathbb{1}[(\boldsymbol{M} \cdot X)_{t+1,\ldots,\ell} = 0] \mid \boldsymbol{M} \in \mathrm{GL}_\ell(\mathbb{F}_q) \setminus M_q^{0,t}(X)] &= 0,
\end{aligned}$$

where the inequality follows from the validity constraints for h.

Thus, we get

$$\begin{aligned}
\mathbb{E}_{\boldsymbol{M} \sim U(\mathrm{GL}_\ell(\mathbb{F}_q))}[(\boldsymbol{M} \cdot X)_1 \cdot \mathbb{1}[(\boldsymbol{M} \cdot X)_{t+1,\ldots,\ell} = 0]] &\leqslant \frac{|M_q^{1,t}(X)| \cdot h(0) - |M_q^{0,t}(X) \setminus M_q^{1,t}(X)|}{|\mathrm{GL}_\ell(\mathbb{F}_q)| \cdot} \\
&= \frac{(t-1)_{r,q} \cdot (1 + h(0)) - (t)_{r,q}}{(\ell)_{r,q}},
\end{aligned}$$

where the equality follows from Lemma 4.4 and (9).

Recalling that our goal is to show (8), we note that

$$\begin{aligned}
&\sum_{t \in [\ell]} (1 + h(0))^{\ell - t} \cdot \mathbb{E}_{\boldsymbol{M} \sim U(\mathrm{GL}_\ell(\mathbb{F}_q))}[(\boldsymbol{M} \cdot X)_1 \cdot \mathbb{1}[(\boldsymbol{M} \cdot X)_{t+1,\ldots,\ell} = 0]] \\
&\quad\leqslant \frac{1}{(\ell)_{r,q}} \sum_{t \in [\ell]} (1 + h(0))^{\ell - t} \cdot ((t-1)_{r,q} \cdot (1 + h(0)) - (t)_{r,q}) \\
&\quad= \frac{(1 + h(0))^\ell \cdot (0)_{r,q} - (\ell)_{r,q}}{(\ell)_{r,q}} = -1,
\end{aligned}$$

where the first equality follows since the sum telescopes. Thus, g is a feasible solution.

It remains to compute the value of g. Note that

$$\begin{aligned}
1 + \sum_{u \in [\ell]} g_u(0) &= 1 + \sum_{t \in [\ell]} (1 + h(0))^{\ell - t} \cdot h(0) \\
&= 1 + \sum_{t \in [\ell]} (1 + h(0))^{\ell - t} \cdot ((1 + h(0)) - 1) = (1 + h(0))^\ell,
\end{aligned}$$

where the last equality follows since the sum telescopes. ■

Remark 4.8. *Note that since the lift in Proposition 4.7 sets all g_u with $u < \ell$ to 0, it follows that this is also a lift of the dual of the full Fourier hierarchy (see Remark 4.3).*

We now prove the more general lift from level k to level ℓ under the assumption that k divides ℓ. We point out that when we take $k = 1$ in Theorem 4.9 below, we recover Proposition 4.7, except for the fact that the constructed solution has coordinates slightly permuted so that it is appropriately compatible with the partial Fourier.

Theorem 4.9. *Let q be a prime power and $k \in \mathbb{N}_+$. If h is a solution of (5) with $\ell = k$ and objective value $V_h \overset{\text{def}}{=} 1 + \sum_{u\in[k]} h_u(0)$, then for every $\ell \in [n]$ divisible by k, letting*

$$g_u(X) \overset{\text{def}}{=} \begin{cases} 0, & \text{if } u \leqslant \ell - k, \\ \displaystyle\sum_{t=0}^{\ell/k-1} V_h^t \cdot h_{u-\ell+k}(X_{\ell-k+1,\ldots,\ell}) \cdot \mathbb{1}[X_{1,\ldots,kt} = 0], & \text{otherwise,} \end{cases}$$

gives a solution of (5) whose objective value is the (ℓ/k)th power of the objective value of h, i.e., we have

$$1 + \sum_{u\in[\ell]} g_u(0) = V_h^{\ell/k} = \left(1 + \sum_{u\in[k]} h_u(0)\right)^{\ell/k}.$$

Proof. Clearly $\mathcal{F}_u(g_u) = 0$ for every $u \in [\ell - k]$. Also, for every $X \in \mathbb{F}_q^{\ell\times n}$, we have

$$\mathcal{F}_\ell(g_\ell)(X) = \sum_{t=0}^{\ell/k-1} V_h^t \cdot \mathcal{F}_{u-\ell+k}(h_{u-\ell+k}(X_{\ell-k+1,\ldots,\ell})) \cdot \mathbb{1}[X_{kt+1,\ldots,\ell-k} = 0] \cdot 2^{-nkt},$$

which is non-negative as $\mathcal{F}_u(h_u) \geqslant 0$ for every $u \in [k]$.

Let us now show the validity constraints. Let $X \in \text{Valid} \setminus \{0\}$ and let $r \overset{\text{def}}{=} \text{rk}(X)$. We need to show that

$$1 + \frac{1}{|\text{GL}_\ell(\mathbb{F}_q)|} \cdot \sum_{u\in[\ell]} (g_u \cdot M)(X) \leqslant 0,$$

which is equivalent to

$$\sum_{t=0}^{\ell/k-1} V_h^t \sum_{u=\ell-k+1}^{\ell} \frac{1}{|\text{GL}_\ell(\mathbb{F}_q)|} \sum_{M\in\text{GL}_\ell(\mathbb{F}_q)} h_{u-\ell+k}((M \cdot X)_{\ell-k+1,\ldots,\ell}) \cdot \mathbb{1}[(M \cdot X)_{1,\ldots,kt} = 0] \leqslant -1.$$

By permuting the rows of the resulting matrix in the expression above, we see that the above is equivalent to

$$\sum_{t=0}^{\ell/k-1} V_h^t \sum_{u\in[k]} \mathbb{E}_{\boldsymbol{M}\sim U(\text{GL}_\ell(\mathbb{F}_q))}[h_u((M \cdot X)_{1,\ldots,k}) \cdot \mathbb{1}[(M \cdot X)_{\ell-kt+1,\ldots,\ell} = 0]] \leqslant -1, \tag{10}$$

where $U(\text{GL}_\ell(\mathbb{F}_q))$ is the uniform distribution on $\text{GL}_\ell(\mathbb{F}_q)$.

To prove the above, fix $t \in \{0, \ldots, \ell/k - 1\}$ and let us study the expression

$$\sum_{u\in[k]} h_u((M \cdot X)_{1,\ldots,k}) \cdot \mathbb{1}[(M \cdot X)_{\ell-kt+1,\ldots,\ell} = 0],$$

where $\boldsymbol{M} \sim U(\mathrm{GL}_\ell(\mathbb{F}_q))$.

First, recalling Definition 4.5, we partition $\mathrm{GL}_\ell(\mathbb{F}_q)$ into the sets

$$M_q^{k,\ell-kt}(X), \qquad M_q^{0,\ell-kt}(X) \setminus M_q^{k,\ell-kt}(X), \qquad \mathrm{GL}_\ell(\mathbb{F}_q) \setminus M_q^{0,\ell-kt}(X),$$

which by Lemmas 4.4 and 4.6 have sizes

$$\begin{gathered}(q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot (\ell - k(t+1))_{r,q} \cdot (\ell - r)!_q, \\ (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot ((\ell - kt)_{r,q} - (\ell - k(t+1))_{r,q}) \cdot (\ell - r)!_q, \\ (q-1)^\ell \cdot q^{\binom{\ell}{2}} \cdot ((\ell)_{r,q} - (\ell - kt))_{r,q}) \cdot (\ell - r)!_q,\end{gathered} \tag{11}$$

respectively.

Note that $\mathbb{1}[(\boldsymbol{M} \cdot X)_{\ell-kt+1,\dots,\ell} = 0]$ only takes non-zero values when $\boldsymbol{M}$ is in one of the first two sets.

Clearly, if we condition on $\boldsymbol{M} \in M_q^{k,\ell-kt}(X)$, then $(\boldsymbol{M} \cdot X)_{1,\dots,k} = 0$.

On the other hand, by Items (i) and (ii) of Lemma 4.6, we know that the conditional distribution of $(\boldsymbol{M} \cdot X)_{1,\dots,k}$ given $\boldsymbol{M} \in M_q^{0,\ell-kt}(X) \setminus M_q^{k,\ell-kt}(X)$ is $\mathrm{GL}_k(\mathbb{F}_q)$-invariant. In particular, this implies that if $\boldsymbol{N} \sim U(\mathrm{GL}_k(\mathbb{F}_q))$ is independent from $\boldsymbol{M}$, then the conditional distributions of $(\boldsymbol{M} \cdot X)_{1,\dots,k}$ and $\boldsymbol{N} \cdot (\boldsymbol{M} \cdot X)_{1,\dots,k}$ given $\boldsymbol{M} \in M_q^{0,\ell-kt}(X) \setminus M_q^{k,\ell-kt}(X)$ are the same. Finally, since $X \in \mathrm{Valid} \setminus \{0\}$, we know that when we condition on $\boldsymbol{M} \in M_q^{0,\ell-kt}(X) \setminus M_q^{k,\ell-kt}(X)$, then $(\boldsymbol{M} \cdot X)_{1,\dots,k}$ is always an element of $\mathrm{Valid} \setminus \{0\}$. Thus we conclude that

$$\sum_{u \in [k]} \mathbb{E}_{\boldsymbol{M}}[h_u((M \cdot X)_{1,\dots,u}) \cdot \mathbb{1}[(M \cdot X)_{\ell-kt+1,\dots,\ell} = 0] \mid \boldsymbol{M} \in M_q^{k,\ell-kt}(X)] = \sum_{u \in [k]} h_u(0) = V_h - 1,$$

$$\begin{aligned}&\sum_{u \in [k]} \mathbb{E}_{\boldsymbol{M}}[h_u((M \cdot X)_{1,\dots,u}) \cdot \mathbb{1}[(M \cdot X)_{\ell-kt+1,\dots,\ell} = 0] \mid \boldsymbol{M} \in M_q^{0,\ell-kt}(X) \setminus M_q^{k,\ell-kt}(X)] \\ &= \sum_{u \in [k]} \mathbb{E}_{\boldsymbol{M}}[\mathbb{E}_{\boldsymbol{N}}[h_u(\boldsymbol{N} \cdot (M \cdot X)_{1,\dots,u}) \cdot \mathbb{1}[(M \cdot X)_{\ell-kt+1,\dots,\ell} = 0]] \mid \boldsymbol{M} \in M_q^{0,\ell-kt}(X) \setminus M_q^{k,\ell-kt}(X)] \\ &\qquad \leqslant -1,\end{aligned}$$

$$\sum_{u \in [k]} \mathbb{E}_{\boldsymbol{M}}[h_u((M \cdot X)_{1,\dots,u}) \cdot \mathbb{1}[(M \cdot X)_{\ell-kt+1,\dots,\ell} = 0] \mid \boldsymbol{M} \in \mathrm{GL}_\ell(\mathbb{F}_q) \setminus M_q^{0,\ell-kt}(X)] = 0,$$

where the inequality follows from the validity constraints for h.

Thus, we get

$$\begin{aligned}&\sum_{u \in [k]} \mathbb{E}_{\boldsymbol{M} \sim U(\mathrm{GL}_\ell(\mathbb{F}_q))}[h_u((M \cdot X)_{1,\dots,u}) \cdot \mathbb{1}[(M \cdot X)_{\ell-kt+1,\dots,\ell} = 0]] \\ &\qquad \leqslant \frac{|M_q^{k,\ell-kt}(X)| \cdot (V_h - 1) - |M_q^{0,\ell-kt}(X) \setminus M_q^{k,\ell-kt}(X)|}{|\mathrm{GL}_\ell(\mathbb{F}_q)|} \\ &\qquad = \frac{(\ell - k(t+1))_{r,q} \cdot V_h - (\ell - kt)_{r,q}}{(\ell)_{r,q}},\end{aligned}$$

where the equality follows from Lemma 4.4 and (11).

Recalling that our goal is to show (8), we note that

$$\begin{aligned}
&\sum_{t=0}^{\ell/k-1} V_h^t \sum_{u\in[k]} \mathbb{E}_{\boldsymbol{M}\sim U(\mathrm{GL}_\ell(\mathbb{F}_q))}[h_u((M\cdot X)_{1,\dots,u})\cdot \mathbb{1}[(M\cdot X)_{\ell-kt+1,\dots,\ell}=0]]\\
&\leqslant \frac{1}{(\ell)_{r,q}}\sum_{t=0}^{\ell/k-1} V_h^t\cdot((\ell-k(t+1))_{r,q}V_h-(\ell-kt)_{r,q})\\
&=\frac{V_h^{\ell/k}\cdot(0)_{r,q}-(\ell)_{r,q}}{(\ell)_{r,q}}=-1,
\end{aligned}$$

where the first equality follows since the sum telescopes. Thus, g is a feasible solution.

It remains to compute the value of g. Note that

$$1+\sum_{u\in[\ell]} g_u(0)=1+\sum_{t=0}^{\ell/k-1} V_h^t\sum_{u=\ell-k+1}^{\ell} h_{u-\ell+k}(0)=1+\sum_{t=0}^{\ell/k-1}V_h^t(V_h-1)=V_h^{\ell/k},$$

where the last equality follows since the sum telescopes. ■

5 Completeness via Subspace Symmetric Dual LPs

We will now give a new proof that the hierarchy is complete, i.e., it recovers the true size of a code at level $\ell\geqslant n$. For this proof, we recall yet another formulation of the hierarchy from [CJJ23].

Instead of symmetrizing (1) under the action of S_n, we recall that $\mathrm{GL}_\ell(\mathbb{F}_q)$ also acts on $\mathbb{F}_q^{\ell\times n}$ by left-multiplication and observe that (1) is also $\mathrm{GL}_\ell(\mathbb{F}_q)$-symmetric. Inspired by terminology from Sum-of-Squares algorithms, given a $\mathrm{GL}_\ell(\mathbb{F}_q)$-symmetric solution f, for each $S\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)$, we define the notation

$$\widetilde{\mathbb{P}}[S\subseteq\widetilde{\boldsymbol{C}}]\stackrel{\text{def}}{=}f(X)$$

for any $X\in\mathbb{F}_q^{\ell\times n}$ with $\mathrm{span}(\{X_1,\dots,X_\ell\})=S$ and interpret this as a pseudo-probability that a pseudo-random variable $\widetilde{\boldsymbol{C}}$ over $L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ contains S. Computing the pseudo-probabilities $\widetilde{\mathbb{P}}[S]\stackrel{\text{def}}{=}\widetilde{\mathbb{P}}[S=\widetilde{\boldsymbol{C}}]$ amounts to a Möbius inversion on the poset $L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ under the inclusion partial order. At levels $\ell\geqslant n$ and when Valid_n is closed under taking subspaces[4], this yields the formulation in (12), whose dual is (13); a code $C\in\mathrm{Valid}_n$ yields a solution $\widetilde{\mathbb{P}}_C[S]\stackrel{\text{def}}{=}\mathbb{1}[S=C]$ of (12), whose value is $|C|^\ell$. The first completeness at levels $\ell\geqslant n$ of [CJJ23] was based on the primal formulation (12) and crucially relied on the fact that non-negative solutions to (12) are convex combinations of true solutions.

[4] It is possible to make this Möbius inversion at lower levels and without the closure under subspaces assumption, but it yields more complicated constraints. Since our completeness result will only hold for levels $\ell\geqslant n$ anyway, we opt for the simpler formulation instead.

$$\boxed{\begin{array}{llll}
\multicolumn{4}{l}{\text{Variables: } (\widetilde{\mathbb{P}}[S] \mid S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n))} \\
\max & \displaystyle\sum_{S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n)} |S|^\ell \widetilde{\mathbb{P}}[S] & & \\
\text{s.t.} & \displaystyle\sum_{S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n)} \widetilde{\mathbb{P}}[S] = 1 & & \text{(Normalization)} \\
& \widetilde{\mathbb{P}}[S] = 0 & \forall S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) \setminus \mathrm{Valid}_n & \text{(Validity)} \\
& \displaystyle\sum_{\substack{S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) \\ S \subseteq U}} |S|^\ell \widetilde{\mathbb{P}}[S] \geqslant 0 & \forall U \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) & \text{(Downward sums)} \\
& \displaystyle\sum_{\substack{S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) \\ U \subseteq S}} \widetilde{\mathbb{P}}[S] \geqslant 0 & \forall U \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) & \text{(Upward sums)}
\end{array}} \tag{12}$$

$$\boxed{\begin{array}{llll}
\multicolumn{4}{l}{\text{Variables: } \alpha \in \mathbb{R}, \beta, \gamma \colon L_{\mathbb{F}_q}(\mathbb{F}_q^n) \to \mathbb{R}} \\
\min & \alpha & & \\
\text{s.t.} & \alpha = |S|^\ell + |S|^\ell \displaystyle\sum_{\substack{T \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) \\ S \leqslant T}} \beta(T) + \sum_{\substack{T \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) \\ T \leqslant S}} \gamma(T) & \forall S \in \mathrm{Valid}_n & \text{(Equality to objective)} \\
& \beta(S) \geqslant 0 & \forall S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) & (\beta \text{ non-negativity}) \\
& \gamma(S) \geqslant 0 & \forall S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) & (\gamma \text{ non-negativity})
\end{array}} \tag{13}$$

It will also be convienient to define for every $k \in \mathbb{N}$ the set

$$\mathrm{Valid}_n^{\dim \leqslant k} \stackrel{\text{def}}{=} \{S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n) \mid \dim_{\mathbb{F}_q}(S) \leqslant k\}.$$

It is clear that for any $\mathrm{Valid}_n \subseteq L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ non-empty, if $k \stackrel{\text{def}}{=} \max\{\dim_{\mathbb{F}_q}(S) \mid S \in \mathrm{Valid}_n\}$, then $\mathrm{Valid}_n \subseteq \mathrm{Valid}_n^{\dim \leqslant k}$. We will show completeness of (13) for valid sets of the form $\mathrm{Valid}_n^{\dim \leqslant k}$ ($k \in \mathbb{N}$) and leverage this to show completeness for arbitrary non-empty valid sets $\mathrm{Valid}_n \subseteq L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ that are closed under taking subspaces. We start with the following key observation.

Key observation: With valid set $\mathrm{Valid}_n^{\dim \leqslant k}$, at completeness levels (i.e., $\ell \geqslant n$), we must have $\alpha = q^{k\ell}$, and, for the dual to achieve this optimum value, many variables $\beta(S)$ and $\gamma(S)$ will need to be zero. This will greatly simplify the dual LP allowing us to establish a recurrence to determine bounds on the remaining variables proving that they can be taken to be nonnegative thereby implying the feasibility of the solution.

Theorem 5.1 (Exact Completeness from the Dual)**.** *For every $\ell \geqslant n$ and every $\mathrm{Valid}_n \subseteq L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ non-empty and closed under taking subspaces, the optimum value of* (13) *is $q^{\ell k}$, where*

$$k \stackrel{\text{def}}{=} \max\{\dim_{\mathbb{F}_q}(S) \mid S \in \mathrm{Valid}_n\}.$$

Proof. Let us make the key observation above formal. First note that since $\mathrm{Valid}_n \subseteq \mathrm{Valid}_n^{\dim \leqslant k}$, it follows that (13) with Valid_n has less constraints than the same program with $\mathrm{Valid}_n^{\dim \leqslant k}$, so it suffices to produce a feasible solution for (13) with $\mathrm{Valid}_n^{\dim\leqslant k}$ whose value is $\alpha \overset{\text{def}}{=} q^{\ell k}$. Since for every $S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ with $\dim_{\mathbb{F}_q}(S) = k$ we have

$$\begin{aligned}\alpha = q^{\ell k} &= |S|^\ell + |S|^\ell \sum_{\substack{T\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)\\ S\subseteq T}} \beta(T) + \sum_{\substack{T\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)\\ T\subseteq S}} \gamma(T)\\ &= |\mathbb{F}_q|^{\ell k} + |\mathbb{F}_q|^{\ell k} \sum_{\substack{T\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)\\ S\subseteq T}} \beta(T) + \sum_{\substack{T\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)\\ T\subseteq S}} \gamma(T)\end{aligned}$$

and both β and γ must be non-negative, we must have $\beta(T) = 0$ whenever $\dim_{\mathbb{F}_q}(T) \geqslant k$ and $\gamma(T) = 0$ whenever $\dim_{\mathbb{F}_q}(T) \leqslant k$.

Let us in fact set $\gamma(T) = 0$ for every $T \in L_{\mathbb{F}_q}(\mathbb{F}_q^n)$. For β, it will be convenient (and sufficient) to consider $\beta(T) = \widetilde{\beta}_{\dim_{\mathbb{F}_q}(T)}$, namely, these variables will only depend on the dimension. Then for a space $S \in L_{\mathbb{F}_q}(\mathbb{F}_q^n)$ of dimension s, the equality to objective constraint reads

$$\begin{aligned}\alpha = q^{\ell k} &= |S|^\ell + |S|^\ell \sum_{i=\dim_{\mathbb{F}_q}(S)}^{n} \sum_{\substack{T\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)\\ S\subseteq T\\ \dim_{\mathbb{F}_q}(T)=i}} \widetilde{\beta}_i\\ &= q^{\ell s} + q^{\ell s} \sum_{i=s}^{k-1} \sum_{\substack{T\in L_{\mathbb{F}_q}(\mathbb{F}_q^n)\\ S\subseteq T\\ \dim_{\mathbb{F}_q}(T)=i}} \widetilde{\beta}_i \qquad\qquad (\text{Since } \widetilde{\beta}_i = 0 \text{ whenever } i \geqslant k.)\\ &= q^{\ell s} + q^{\ell s} \sum_{i=s}^{k-1} \binom{n-s}{i-s}_q \widetilde{\beta}_i.\end{aligned}$$

Thus, to satisfy all equality to objective constraints, the following recurrence must hold for every $s \in \{0, \ldots, k-1\}$:

$$\widetilde{\beta}_s = q^{\ell(k-s)} - 1 - \sum_{i=s+1}^{k-1} \binom{n-s}{i-s}_q \widetilde{\beta}_i. \tag{14}$$

Our objective is then to prove by reverse induction in $s \in \{0, \ldots, k-1\}$ that defining $\widetilde{\beta}$ by (14) above yields $\widetilde{\beta}_s \geqslant 0$ for every $s \in \{0, \ldots, k-1\}$.

First note that (14) for $s = k-1$ yields $\widetilde{\beta}_{k-1} = q^\ell - 1 \geqslant 0$. Suppose now that $s \in \{0, \ldots, k-2\}$ and note that using (14) for $\widetilde{\beta}_{s+1}$ in its version for $\widetilde{\beta}_s$, we get

$$\begin{aligned}\widetilde{\beta}_s &= q^{\ell(k-s)} - 1 - \sum_{i=s+2}^{k-1} \binom{n-s}{i-s}_q \widetilde{\beta}_i - \binom{n-s}{1}_q \left(q^{\ell(k-s-1)} - 1 - \sum_{i=s+2}^{k-1} \binom{n-s-1}{i-s-1}_q \widetilde{\beta}_i \right)\\ &= q^{\ell(k-s)} \left(1 - \frac{[n-s]_q}{q^\ell} \right) + [n-s]_q - 1 + \sum_{i=s+2}^{k-1} \left([n-s]_q \binom{n-s-1}{i-s-1}_q - \binom{n-s}{i-s}_q \right) \widetilde{\beta}_i \quad \geqslant 0,\end{aligned}$$

where the inequality follows since

$$\begin{aligned}
1 - \frac{[n-s]_q}{q^\ell} &\geqslant 1 - q^{n-s-\ell} \geqslant 0 && \text{(since } \ell \geqslant n\text{)},\\
[n-s]_q - 1 &\geqslant 0 && \text{(since } s \leqslant k-2 < n\text{)},\\
[n-s]_q \binom{n-s-1}{i-s-1}_q - \binom{n-s}{i-s}_q &= \binom{n-s}{i-s}_q ([i-s]_q - 1) \geqslant 0 && \text{(for every } i \geqslant s+2\text{)},
\end{aligned}$$

and since inductively we have $\widetilde{\beta}_i \geqslant 0$ for every $i \geqslant s+2$.

Thus, we conclude that setting

$$\alpha \overset{\text{def}}{=} q^{\ell k}, \qquad \beta(T) \overset{\text{def}}{=} \widetilde{\beta}_{\dim_{\mathbb{F}_q}(T)}, \qquad \gamma(T) \overset{\text{def}}{=} 0,$$

(where $\widetilde{\beta}_s$ is given recursively by (14) for $s \in \{0, \ldots, k-1\}$ and is zero when $s \geqslant k$) yields a feasible solution of (13) (for both Valid_n and $\mathrm{Valid}_n^{\dim \leqslant k}$) whose value is $q^{\ell k}$. ■

6 Spectral-based Dual solutions for Balanced codes

In this section, we construct a spectral-based solution at level ℓ for ε-balanced codes over $\mathbb{F}_2$ whose values are comparable with the MRRW solution. The set of *(linear) ε-balanced codes (over $\mathbb{F}_2^n$)* is defined as

$$\mathrm{Valid}_n^\varepsilon \overset{\text{def}}{=} \left\{ C \in L_{\mathbb{F}_2}(\mathbb{F}_2^n) \;\middle|\; \forall x \in C \setminus \{0\}, \left((1-\varepsilon)\frac{n}{2} \leqslant |x| \leqslant (1+\varepsilon)\frac{n}{2} \right) \right\},$$

so we have

$$\mathrm{Valid}_{n,\ell}^\varepsilon = \left\{ X \in \mathbb{F}_2^{\ell \times n} \;\middle|\; \forall u \in \mathbb{F}_2^\ell, \left(uX \neq 0 \to \left((1-\varepsilon)\frac{n}{2} \leqslant |uX| \leqslant (1+\varepsilon)\frac{n}{2} \right) \right) \right\}.$$

We recall that for an ε-balanced code, the MRRW bound on the rate is of the form

$$\frac{1+o(1)}{4}\varepsilon^2 \lg \frac{1}{\varepsilon} + O_\varepsilon\left(\frac{\lg(n)}{n}\right) \tag{15}$$

as $n \to \infty$ and $\varepsilon \to 0$ (in the above, the error term $O_\varepsilon(\lg(n)/n)$ hides multiplicative factors dependent on ε, but the error term $o(1)$ only hides multiplicative factors that do not depend on n nor on ε). We will retrieve this bound on every constant level of the hierarchy. However, we point out right away that the error terms hidden are slightly worse than the MRRW bound and get worse as the level increases.

Recall that the LP (2) is symmetric under the action of S_n, and so is the solution we construct. Namely, it is constant on the orbits $\mathbb{F}_2^{\ell \times n}/S_n$. As it turns out, S_n-orbits can be characterized in terms of *configurations*, defined below in (16). In Section 6.1 we develop the language and tools necessary to work with symmetric functions.

In Section 6.2 we construct a family of feasible solutions of the form[5]

$$f(X) \overset{\text{def}}{=} \frac{\Phi_m(X) \cdot \widehat{\Lambda}^2(X)}{(\widehat{\Phi}_m * \Lambda * \Lambda)(0)},$$

[5] In Section 3, we used the notation Γ which relates to Λ by $\Gamma = \widehat{\Lambda}$, up to a positive multiplicative factor.

where Φ_m is non-positive on $X \in \mathrm{Valid}^{\varepsilon}_{n,\ell}$, and $\Lambda(X) \overset{\mathrm{def}}{=} \mathbb{1}[\mathrm{config}_{n,\ell}(X) = h]$ for some $h \in \mathrm{Config}_{n,\ell}$.

The definition of Φ_m is given in (20), and its necessary properties in Lemma 6.6. It can be viewed, informally, as the product of $2^\ell - 1$ cylinders in $\mathbb{R}^{\mathbb{F}_2^\ell \setminus \{0\}}$ (see Figs. 1 to 6). Each cylinder is negative on the inside and positive on the outside. The cylinders are centered and rotated so that every $X \in \mathrm{Valid}^{\varepsilon}_{n,\ell}$ is inside an odd number of cylinders, and hence $\Phi_m(X) \leqslant 0$.

In Theorem 6.7 we prove that the construction yields a feasible solution, given that Λ satisfies certain conditions. The theorem also provides an upper bound on the objective value attained by this construction, and hence on $|C|^\ell$ for $C \in \mathrm{Valid}_n$.

Finally, in Section 6.3 we find a satisfactory Λ by choosing a configuration $h \in \mathrm{Config}_{n,\ell}$, and showing that it satisfies Theorem 6.7 and gives the correct value.

6.1 Basic definitions and properties

This section is dedicated to basic definitions and properties working up to Lemma 6.4, which provides an easier formula for the action of powers of the matrix A_v defined below.

For $X \in \mathbb{F}_q^{\ell \times n}$, the *(Venn diagram) configuration* of X is the function $\mathrm{config}_{n,\ell}(X) \colon \mathbb{F}_q^\ell \to \mathbb{N}$ given by letting for each $u \in \mathbb{F}_q^\ell$

$$\mathrm{config}_{n,\ell}(X)(u) \overset{\mathrm{def}}{=} |\{k \in [n] \mid \forall j \in [\ell], X_{jk} = u_j\}|$$

be the number of columns of X that are equal to u. It is straightforward to check that two elements X and Y of $\mathbb{F}_q^{\ell \times n}$ are in the same S_n-orbit if and only if $\mathrm{config}_{n,\ell}(X) = \mathrm{config}_{n,\ell}(Y)$. The set of all configurations is denoted by

$$\mathrm{Config}_{n,\ell} \overset{\mathrm{def}}{=} \mathrm{config}_{n,\ell}(\mathbb{F}_q^{\ell \times n}) = \{g \colon \mathbb{F}_q^\ell \to \mathbb{N} \mid \sum_{u \in \mathbb{F}_q^\ell} g(u) = n\}. \tag{16}$$

It will be convenient to use the set

$$\mathrm{NConfig}_\ell \overset{\mathrm{def}}{=} \left\{ G \colon \mathbb{F}_2^\ell \to \mathbb{R}_+ \;\middle|\; \sum_{v \in \mathbb{F}_2^\ell} G(v) = 1 \right\}$$

of normalized Venn diagram configurations over $\mathbb{F}_2$ (note that we can naturally interpret elements of $\mathrm{NConfig}_\ell$ as probability distributions on $\mathbb{F}_2^\ell$).

For $h \in \mathrm{Config}_{n,\ell}$, we let $A_h \in \mathbb{R}^{\mathbb{F}_2^{\ell \times n} \times \mathbb{F}_2^{\ell \times n}}$ and $L_h \in \mathbb{R}^{\mathbb{F}_2^{\ell \times n}}$ be given by

$$A_h(x, y) \overset{\mathrm{def}}{=} \mathbb{1}[\mathrm{config}_{n,\ell}(x - y) = h], \qquad L_h(x) \overset{\mathrm{def}}{=} 2^{n\ell}\mathbb{1}[\mathrm{config}_{n,\ell}(x) = h],$$

and note that

$$A_h \Lambda = L_h * \Lambda.$$

For every $u \in \mathbb{F}_2^\ell \setminus \{0\}$, define $h_u \in \mathrm{Config}_{n,\ell}$ by

$$h_u(v) \overset{\mathrm{def}}{=} \begin{cases} 1, & \text{if } u = v, \\ n - 1, & \text{if } u = 0, \\ 0, & \text{otherwise,} \end{cases}$$

and define the shorthand notations $A_u \overset{\mathrm{def}}{=} A_{h_u}$ and $L_u \overset{\mathrm{def}}{=} L_{h_u}$.

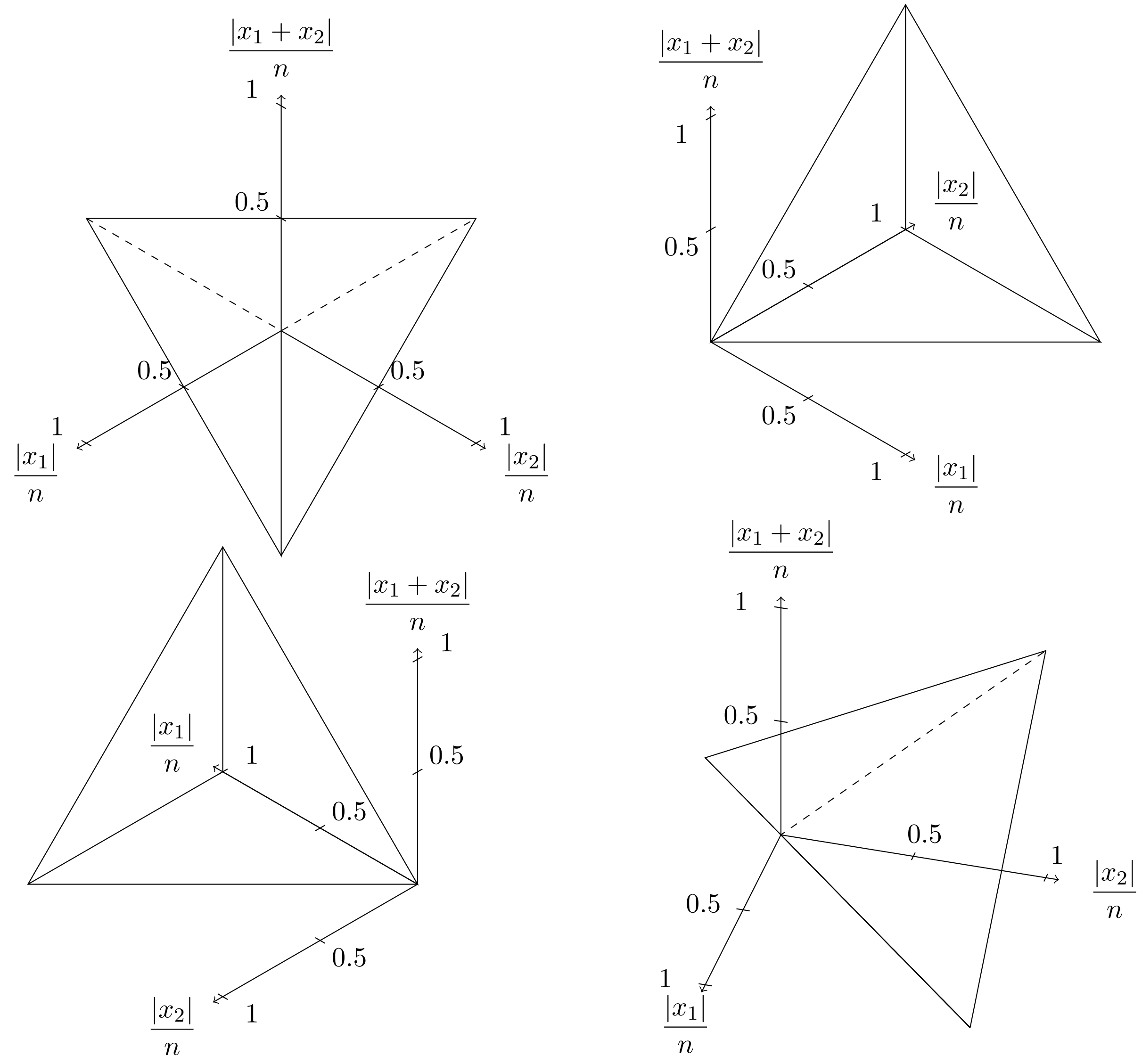


Figure 1: Different projections of the space of all possible Hamming weight combinations when $\ell = 2$ (the picture rescales n out). Three of the six edges of the tetrahedron are contained on the coordinate planes. The top left projection is isometric.

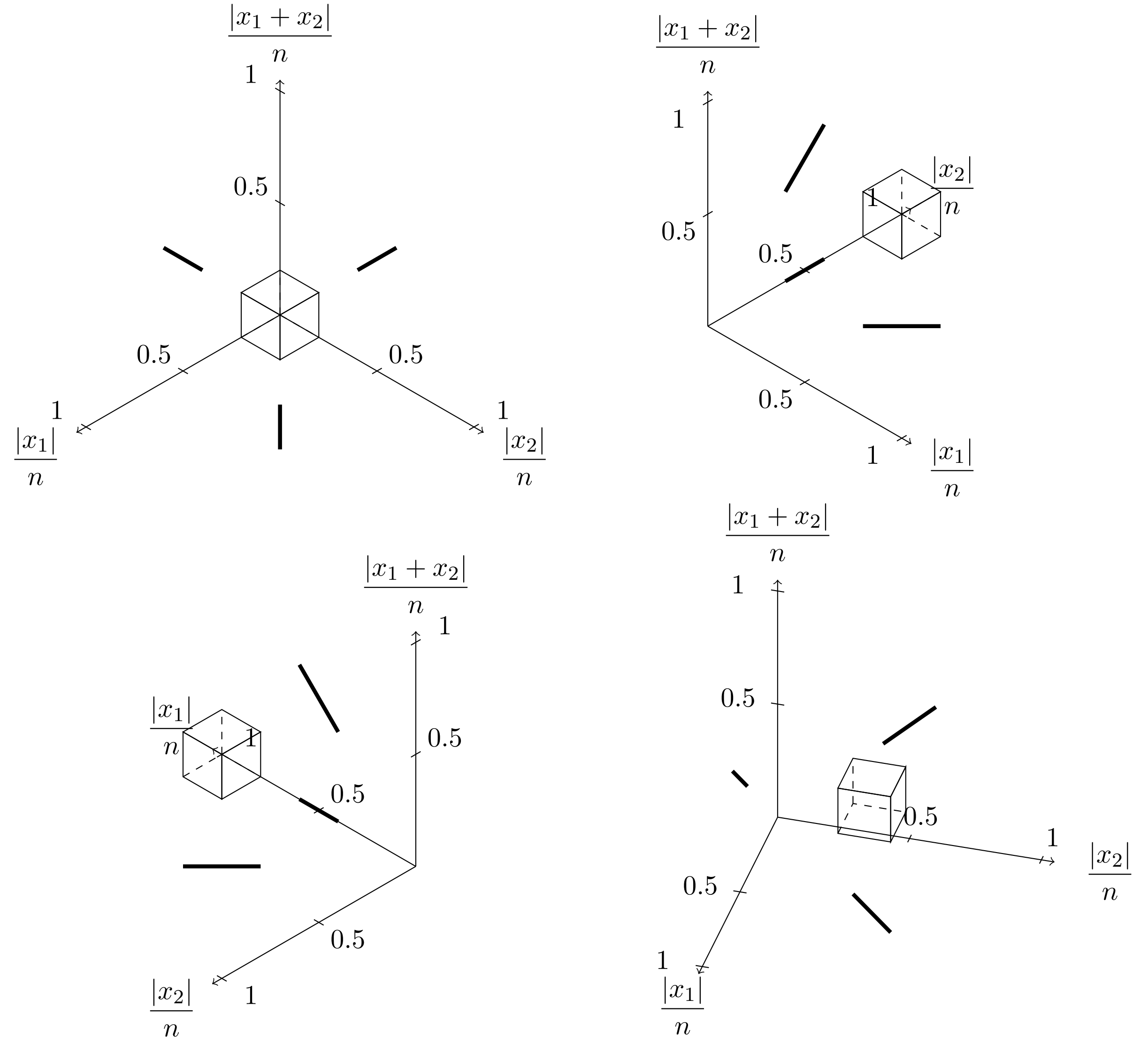


Figure 2: Different projections of $\mathrm{Valid}^{\varepsilon}_{n,\ell}$ (in Hamming weight coordinates) with $\varepsilon = 0.2$ (the picture rescales n out) when $\ell = 2$. The region $\mathrm{Valid}_{n,\varepsilon}$ consists of the origin, the three line segments on the coordinate planes and the cube (with interior) in the middle. The cube faces are paralel to the coordinate planes. The top left projection is isometric.

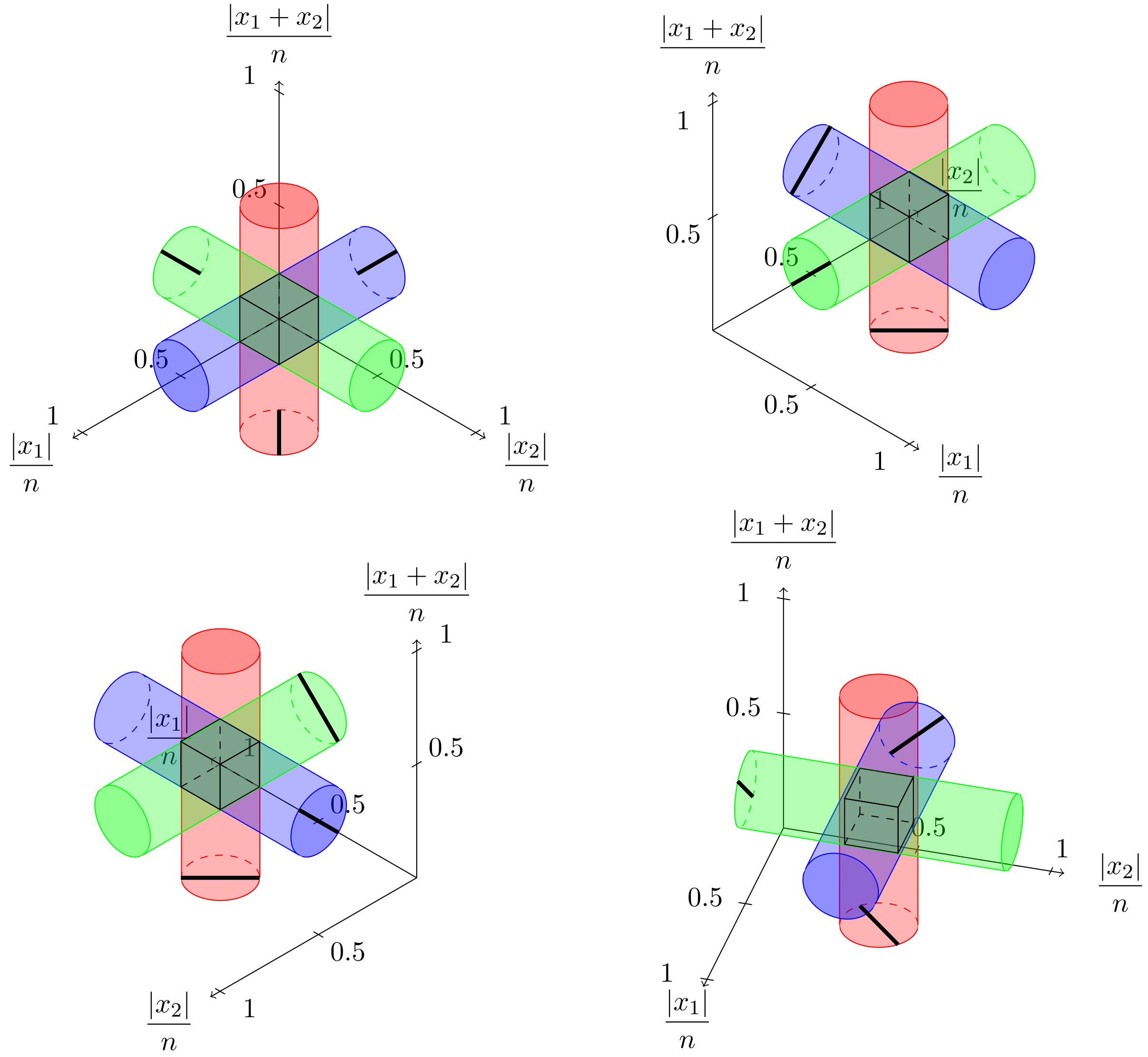


Figure 3: Different projections of $\mathrm{Valid}^{\varepsilon}_{n,\ell}$ (in Hamming weight coordinates) with $\varepsilon = 0.2$ (the picture rescales n out) and the cylinders when $\ell = 2$. The region $\mathrm{Valid}_{n,\varepsilon}$ consists of the origin, the three line segments on the coordinate planes and the cube (with interior) in the middle. The vertices of the cube are precisely the points in which all three cylinder surfaces intersect. The cube faces and cylinder bases are parallel to the coordinate plane. The top left projection is isometric.

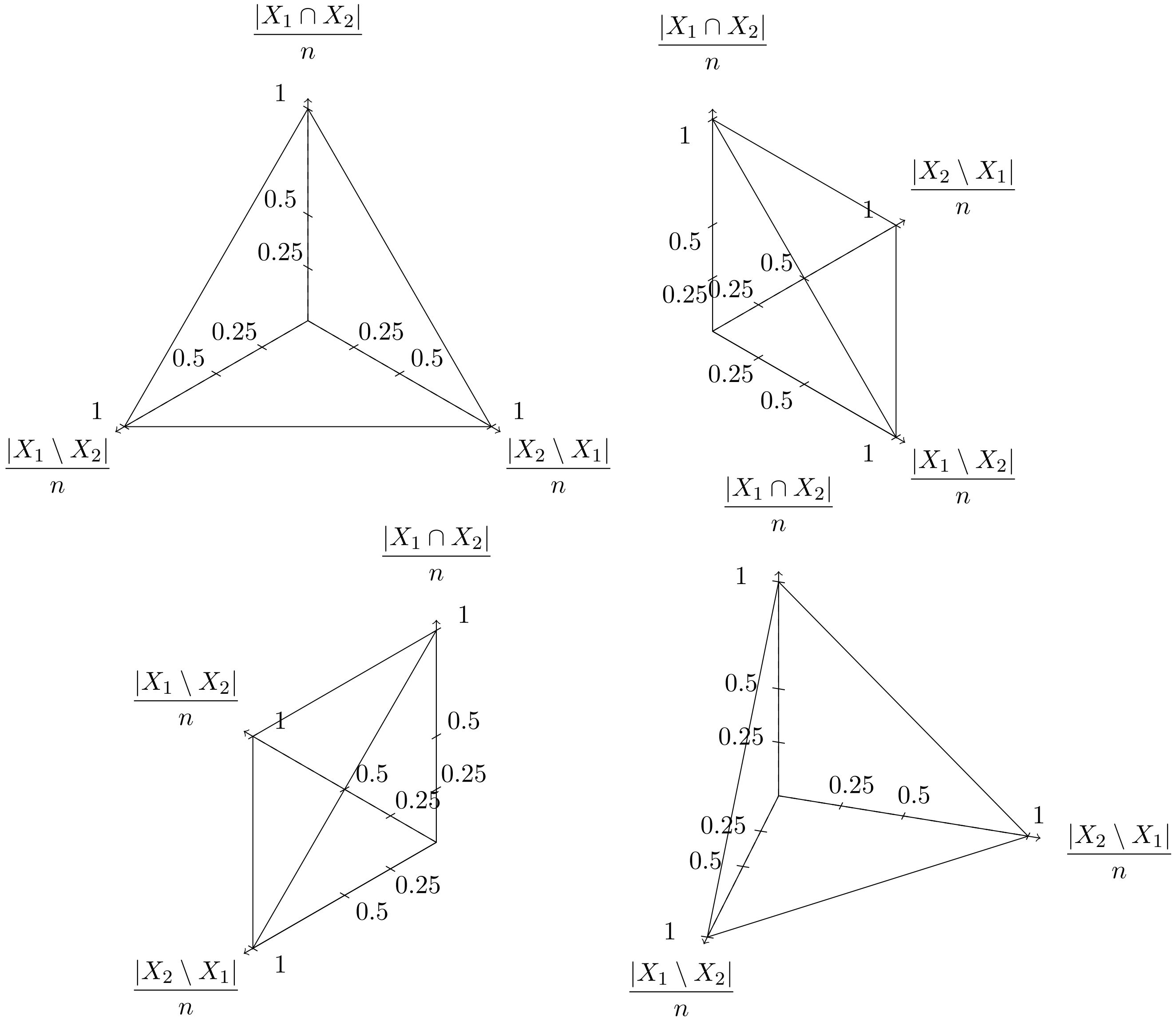
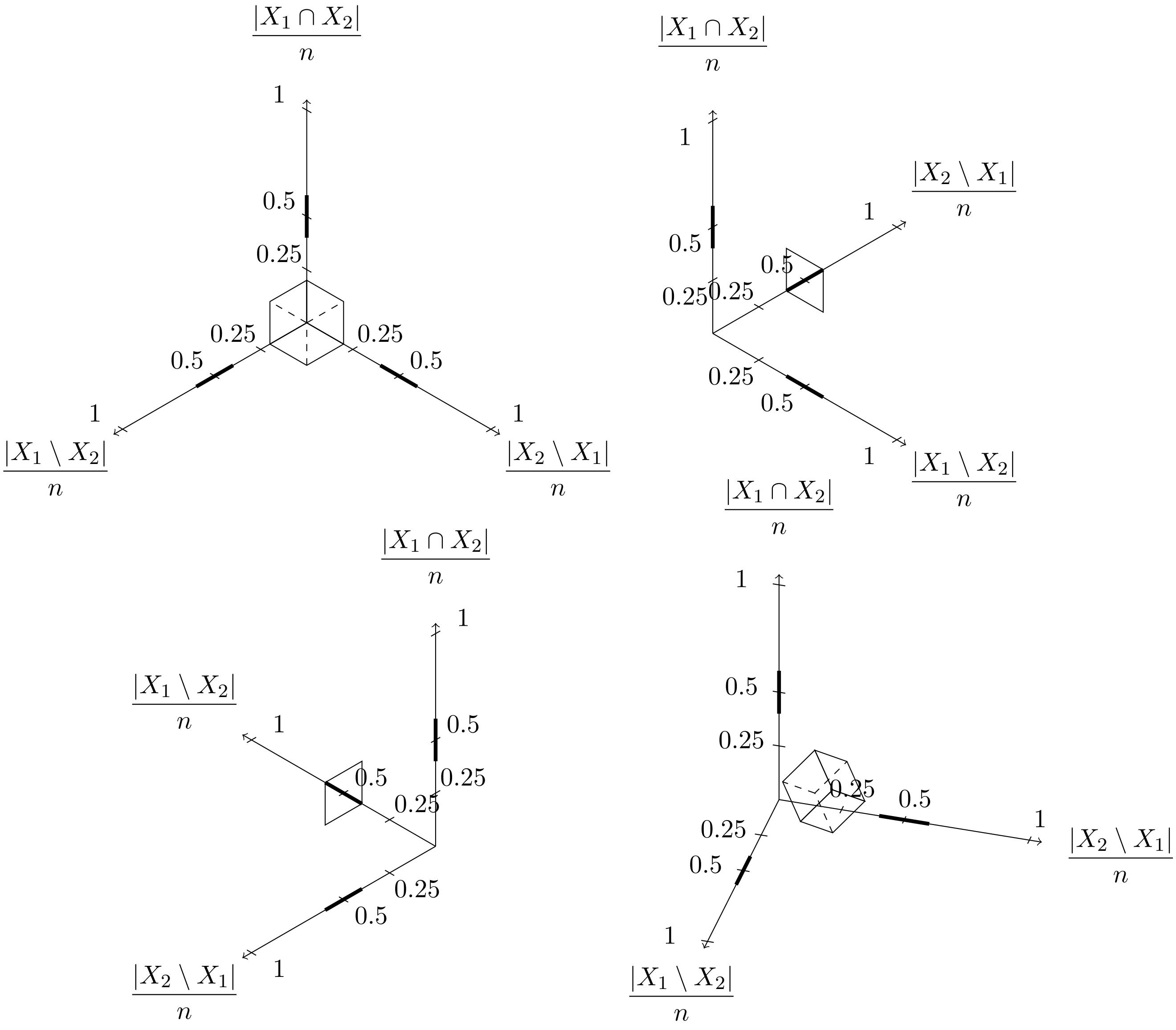
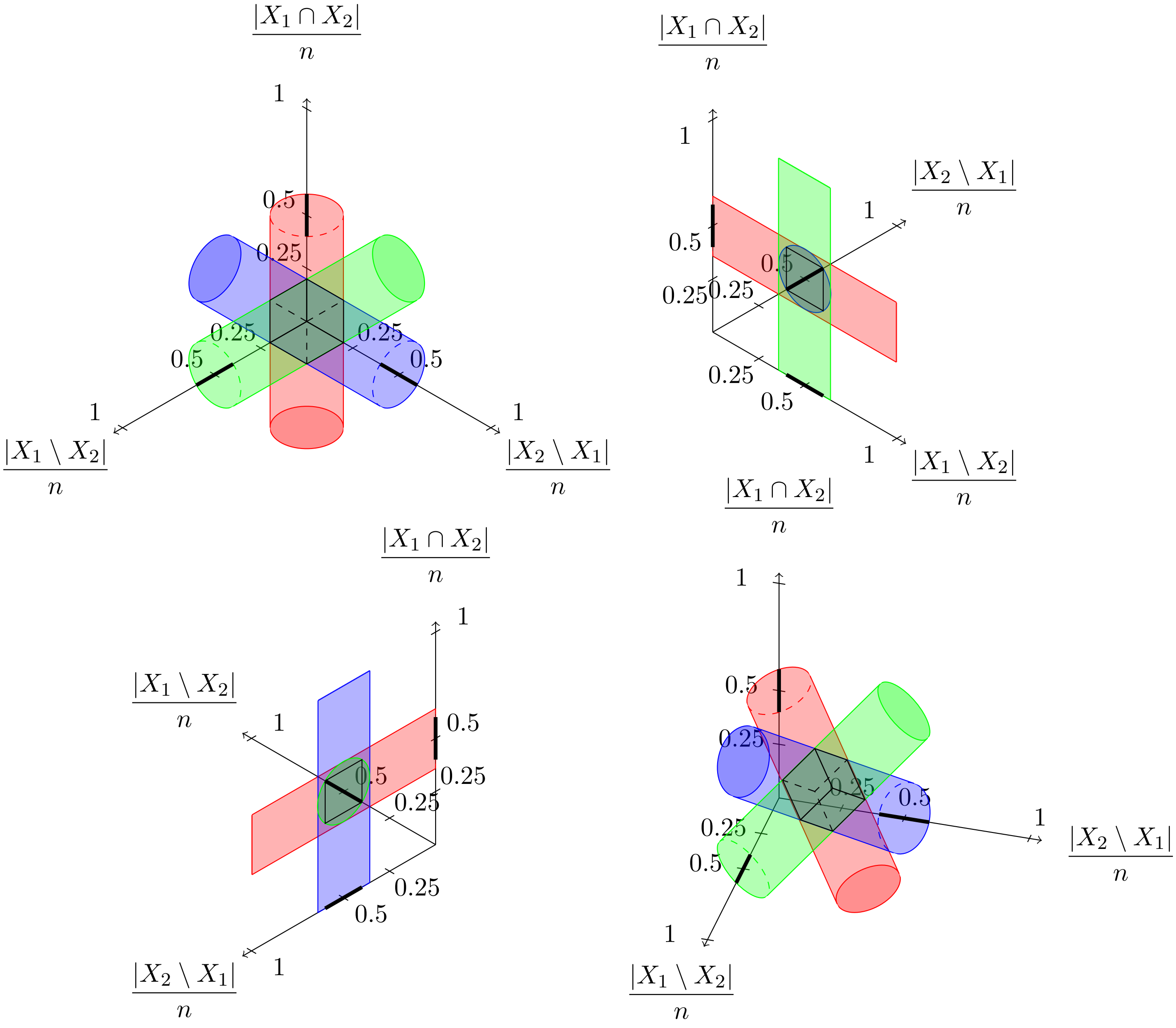

$\frac{|X_1 \cap X_2|}{n}$
1
0.5
0.25
0.25
0.5
0.25
0.5
1
1
$\frac{|X_1 \setminus X_2|}{n}$
$\frac{|X_2 \setminus X_1|}{n}$
$\frac{|X_1 \cap X_2|}{n}$
1
$\frac{|X_2 \setminus X_1|}{n}$
1
0.5
0.5
0.25
0.25
0.25
0.5
1
$\frac{|X_1 \setminus X_2|}{n}$
$\frac{|X_1 \cap X_2|}{n}$
1
$\frac{|X_1 \setminus X_2|}{n}$
1
0.5
0.5
0.25
0.25
0.25
0.5
$\frac{|X_2 \setminus X_1|}{n}$
1
$\frac{|X_1 \cap X_2|}{n}$
1
0.5
0.25
0.25
0.5
1
$\frac{|X_2 \setminus X_1|}{n}$
0.25
0.5
1
$\frac{|X_1 \setminus X_2|}{n}$

Figure 4: Different projections of the space of all possible Venn diagram configurations when $\ell = 2$ (the picture rescales n out). Three of the tetrahedron faces are on coordinate planes. The top left projection is isometric.



$\frac{|X_1 \cap X_2|}{n}$
1
0.5
0.25
0.25
0.5
1
$\frac{|X_1 \setminus X_2|}{n}$
0.25
0.5
1
$\frac{|X_2 \setminus X_1|}{n}$
$\frac{|X_1 \cap X_2|}{n}$
1
0.5
0.25
0.25
0.5
1
$\frac{|X_2 \setminus X_1|}{n}$
0.25
0.5
1
$\frac{|X_1 \setminus X_2|}{n}$
$\frac{|X_1 \cap X_2|}{n}$
1
$\frac{|X_1 \setminus X_2|}{n}$
1
0.5
0.5
0.25
0.25
0.25
0.5
1
$\frac{|X_2 \setminus X_1|}{n}$
$\frac{|X_1 \cap X_2|}{n}$
1
0.5
0.25
0.25
0.5
1
$\frac{|X_2 \setminus X_1|}{n}$
0.25
0.5
1
$\frac{|X_1 \setminus X_2|}{n}$

Figure 5: Different projections of $\text{Valid}^{\varepsilon}_{n,\ell}$ in Venn diagram configuration space with $\varepsilon = 0.2$ (the picture rescales n out) when $\ell = 2$. Here $X_i \overset{\text{def}}{=} \text{supp}(x_i)$. The region $\text{Valid}_{n,\varepsilon}$ consists of the origin, the three line segments on the coordinate axes and the cube (with interior) in the middle. None of the cube faces are parallel to the coordinate planes. The top left projection is isometric. On the top right and bottom left projections, two of the cube faces are parallel to the projection plane.



$\frac{|X_1 \cap X_2|}{n}$
1
0.5
0.25
0.25
0.25
0.5
0.5
1
1
$\frac{|X_1 \setminus X_2|}{n}$
$\frac{|X_2 \setminus X_1|}{n}$
$\frac{|X_1 \cap X_2|}{n}$
1
$\frac{|X_2 \setminus X_1|}{n}$
1
0.5
0.5
0.25
0.25
0.25
0.5
1
$\frac{|X_1 \setminus X_2|}{n}$
$\frac{|X_1 \cap X_2|}{n}$
1
$\frac{|X_1 \setminus X_2|}{n}$
1
0.5
0.5
0.25
0.25
0.25
0.5
$\frac{|X_2 \setminus X_1|}{n}$
1
$\frac{|X_1 \cap X_2|}{n}$
1
0.5
0.25
0.25
0.5
1
$\frac{|X_2 \setminus X_1|}{n}$
0.25
0.5
1
$\frac{|X_1 \setminus X_2|}{n}$

Figure 6: Different projections of $\mathrm{Valid}^{\varepsilon}_{n,\ell}$ (in Venn diagram configuration) with $\varepsilon = 0.2$ (the picture rescales n out) and the cylinders when $\ell = 2$. Here $X_i \overset{\mathrm{def}}{=} \mathrm{supp}(x_i)$. The region $\mathrm{Valid}_{n,\varepsilon}$ consists of the origin, the three line segments on the coordinate axes and the cube (with interior) in the middle. The vertices of the cube are precisely the points in which all three cylinder surfaces intersect. None of the cube faces or cylinder bases are parallel to the coordinate planes and none of the cylinder axes are parallel to any coordinate axes. The top left projection is isometric. On the top right and bottom left projections, two of the cube faces are parallel to the projection plane and two of the slanted cylinders have their bases appearing degenerate due to the projection and the other has its axis orthogonal to the projection.

Lemma 6.1. *For $\ell, n \in \mathbb{N}_+$ and $g \in \mathrm{Config}_{n,\ell}$, we have*

$$|\mathrm{config}_{n,\ell}^{-1}(g)| = \binom{n}{g}.$$

In particular, if $G \in \mathrm{NConfig}_\ell$ is such that $G(u) > 0$ for every $u \in \mathbb{F}_2^\ell$ and $n \cdot G \in \mathrm{Config}_{n,\ell}$, then

$$|\mathrm{config}_{n,\ell}^{-1}(n \cdot G)| = (1 + o(1)) \cdot \sqrt{\frac{(2\pi n)^{(1-2^\ell)}}{\prod_{u\in\mathbb{F}_2^\ell} G(u)}} \cdot 2^{H_2(G)\cdot n}$$

as $n \to \infty$ with ℓ fixed, where $H_2(G)$ is the binary entropy of G (as a probability distribution over $\mathbb{F}_2^\ell$).

Proof. By definition, every $X \in \mathrm{config}_{n,\ell}^{-1}(g)$ must be such that for every $u \in \mathbb{F}_2^\ell$, exactly $g(u)$ of the n columns of X must be equal to u. Thus, we conclude that

$$|\mathrm{config}_{n,\ell}^{-1}(g)| = \binom{n}{g} = \frac{n!}{\prod_{u\in\mathbb{F}_2^\ell} g(u)!}.$$

Finally, if $G \in \mathrm{NConfig}_\ell$ is such that $G(u) > 0$ for every $u \in \mathbb{F}_2^\ell$ and $n \cdot G \in \mathrm{Config}_{n,\ell}$, then

$$\begin{aligned}|\mathrm{config}_{n,\ell}^{-1}(n \cdot G)| = \binom{n}{n \cdot G} &= (1 + o(1)) \cdot \sqrt{\frac{(2\pi n)^{(1-2^\ell)}}{\prod_{u\in\mathbb{F}_2^\ell} G(u)}} \cdot \frac{1}{\prod_{u\in\mathbb{F}_2^\ell} G(u)^{G(u)\cdot n}} \\ &= (1 + o(1)) \cdot \sqrt{\frac{(2\pi n)^{(1-2^\ell)}}{\prod_{u\in\mathbb{F}_2^\ell} G(u)}} \cdot 2^{H_2(G)\cdot n},\end{aligned}$$

where the second equality follows from Stirling's Approximation. ■

Lemma 6.2. *Let $g, h \in \mathrm{Config}_{n,\ell}$ and let*

$$\mathcal{F}_{g,h} \overset{\text{def}}{=} \left\{ F \colon \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell \to \mathbb{N} \;\middle|\; \sum_{u\in\mathbb{F}_2^\ell} F(u, -) = g \wedge \sum_{v\in\mathbb{F}_2^\ell} F(-, v) = h \right\}. \tag{17}$$

Then the following hold for $Y \in \mathrm{config}_{n,\ell}^{-1}(g)$.

i. For every $X \in \mathrm{config}_{n,\ell}^{-1}(h)$, let $F_X \colon \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell \to \mathbb{N}$ be given by letting

$$F_X(u, v) \overset{\text{def}}{=} |\{k \in [n] \mid \forall j \in [\ell], (X_{jk} = u_j \wedge Y_{jk} = v_j)\}| \tag{18}$$

be the number of indices $k \in [n]$ such that the kth column of X is u and the kth column of Y is v. Then $F_X \in \mathcal{F}_{g,h}$.

ii. For $F \in \mathcal{F}_{g,h}$, we have

$$|\{X \in \mathrm{config}_{n,\ell}^{-1}(h) \mid F_X = F\}| = \prod_{v\in\mathbb{F}_2^\ell} \binom{g(v)}{F(-, v)},$$

where F_X is given by (18).

Proof. Item (i) follows since for every $v \in \mathbb{F}_2^\ell$, we have

$$\sum_{u \in \mathbb{F}_2^\ell} F_X(u,v) = |\{k \in [n] \mid \forall j \in [\ell], Y_{jk} = v_j\}| = \mathrm{config}_{n,\ell}(Y)(v) = g(v)$$

and for every $u \in \mathbb{F}_2^\ell$, we have

$$\sum_{v \in \mathbb{F}_2^\ell} F_x(u,v) = |\{k \in [n] \mid \forall j \in [\ell], X_{jk} = u_j\}| = \mathrm{config}_{n,\ell}(X)(u) = h(u).$$

For Item (ii), we note that to count the number of $X \in \mathrm{config}_{n,\ell}^{-1}(h)$ with $F_X = F$, we consider $[n]$ partitioned naturally into 2^ℓ parts indexed by $v \in \mathbb{F}_2^\ell$ as

$$P_v \overset{\text{def}}{=} \{k \in [n] \mid \forall j \in [\ell], Y_{jk} = v_j\}$$

and note that to get $F_X = F$ for each $u \in \mathbb{F}_2^\ell$, we must have exactly $F(u,v)$ elements of P_v in

$$\{k \in [n] \mid \forall j \in [\ell], (X_{jk} = u_j \wedge Y_{jk} = v_j)\},$$

since the above are pairwise disjoint and $|P_v| = g(v)$, we conclude that the number of such choices amounts to the multinomial

$$\binom{g(v)}{F(-,v)}$$

(recall that $\sum_{u \in \mathbb{F}_2^\ell} F(u,v) = g(v)$, so the multinomial above is non-zero). Since all such choices are independent for the different $v \in \mathbb{F}_2^\ell$, we conclude that

$$|\{X \in \mathrm{config}_{n,\ell}^{-1}(h) \mid F_X = F\}| = \prod_{v \in \mathbb{F}_2^\ell} \binom{g(v)}{F(-,v)},$$

as desired. ■

Lemma 6.3. *Let* $\Psi\colon \mathrm{Config}_{n,\ell} \to \mathbb{R}$, *let* $\psi \overset{\text{def}}{=} \Psi \circ \mathrm{config}_{n,\ell}$, *let* $g, h \in \mathrm{Config}_{n,\ell}$ *and let* $Y \in \mathrm{config}_{n,\ell}^{-1}(g)$. *Then*

$$A_h \psi(Y) = \sum_{F \in \mathcal{F}_{g,h}} \prod_{w \in \mathbb{F}_2^\ell} \binom{g(w)}{F(-,w)} \Psi(g + \Delta_F),$$

where $\mathcal{F}_{g,h}$ *is given by* (17) *and*

$$\Delta_F(v) \overset{\text{def}}{=} \sum_{u \in \mathbb{F}_2^\ell} (F(u, u+v) - F(u,v)).$$

Proof. First note that

$$A_h \psi(Y) = \sum_{\substack{Z \in \mathbb{F}_2^{\ell \times n} \\ \mathrm{config}_{n,\ell}(Z-Y) = h}} \psi(Z) = \sum_{X \in \mathrm{config}_{n,\ell}^{-1}(h)} \psi(X+Y).$$

We now split the sum above based on the joint configuration of X and Y, that is, for $X \in \mathrm{config}_{n,\ell}^{-1}(h)$, we let $F_X\colon \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell \to \mathbb{N}$ be given by (18), i.e., we have

$$F_X(u,v) \overset{\text{def}}{=} |\{k \in [n] \mid \forall j \in [\ell], (X_{jk} = u_j \wedge Y_{jk} = v_j)\}|.$$

Note that sets in the above partition $[n]$ naturally into $2^\ell \times 2^\ell$ parts indexed by $(u,v) \in \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell$. Recalling that $\mathrm{config}_{n,\ell}(Y) = g$, we note that

$$\begin{aligned}
\mathrm{config}_{n,\ell}(X+Y)(v) &= |\{k \in [n] \mid \forall j \in [\ell], (X+Y)_{jk} = v_j\}| \\
&= \sum_{u \in \mathbb{F}_2^\ell} |\{k \in [n] \mid \forall j \in [\ell], (X_{jk} = u_j \wedge Y_{jk} = u_j + v_j)\}| \\
&= g(v) + \Delta_F(v),
\end{aligned}$$

where the last equality follows since $\sum_{u \in \mathbb{F}_2^\ell} F(u,v) = g(v)$. ■

Lemma 6.4. *Let $v \in \mathbb{F}_2^\ell \setminus \{0\}$ and $g_0 \in \mathrm{Config}_{n,\ell}$ be such that for every $u \in \mathbb{F}_2^\ell$, if $g_0(u) \neq 0$, then $g_0(u) \geqslant \Omega(n)$. Let also $\Lambda \overset{\text{def}}{=} \mathbb{1}_{\mathrm{config}_{n,\ell}^{-1}(g_0)}$ and $X \in \mathrm{config}_{n,\ell}^{-1}(g_0)$.*

Then

$$A_v^m \Lambda(X) = \sum_{F \in \mathcal{F}_{m,v}} \binom{m}{F} \prod_{u \in \mathbb{F}_2^\ell} g_0(u)^{F(u)} + o(n^m),$$

as $n \to \infty$ with m and ℓ fixed, where

$$\mathcal{F}_{m,v} \overset{\text{def}}{=} \left\{ F\colon \mathbb{F}_2^\ell \to \mathbb{N} \;\middle|\; \sum_{u \in \mathbb{F}_2^\ell} F(u) = m \wedge \forall u \in \mathbb{F}_2^\ell, F(u+v) = F(u) \right\}. \tag{19}$$

Proof. Applying Lemma 6.3 for the particular case when $h = h_v$, every $F \in \mathcal{F}_{g,h}$ is of the form $F = F_t$ for some $t \in \mathbb{F}_2^\ell$, where

$$F_t(u,w) \overset{\text{def}}{=} \begin{cases} 1, & \text{if } u = v \text{ and } w = t, \\ g(t) - 1, & \text{if } u = 0 \text{ and } w = t, \\ g(w), & \text{if } u = 0 \text{ and } w \neq t, \\ 0, & \text{otherwise.} \end{cases}$$

Furthermore, note that we have $\Delta_{F_t} = \mathbb{1}_{\{v+t\}} - \mathbb{1}_{\{t\}}$ and

$$\prod_{w \in \mathbb{F}_2^\ell} \binom{g(w)}{F_t(-,w)} = g(t).$$

Thus we have

$$A_v \psi(Y) = \sum_{t \in \mathbb{F}_2^\ell} g(t) \Psi(g + \mathbb{1}_{\{v+t\}} - \mathbb{1}_{\{t\}})$$

and with a simple induction, we have

$$A_v^m \psi(Y) = \sum_{t \in T_m(g)} \left(\prod_{j=1}^{m} g_{t,j-1}(t_j) \right) \Psi(g_{t,m}),$$

where

$$g_{t,j} \overset{\text{def}}{=} g + \sum_{k=1}^{j-1} (\mathbb{1}_{\{v+t_k\}} - \mathbb{1}_{\{t_k\}}),$$

$$T_m(g) \overset{\text{def}}{=} \{t \in (\mathbb{F}_2^\ell)^m \mid \forall j \in [m], g_{t,j} \in \mathrm{Config}_{n,\ell}, g_{t,j-1}(t_j) \neq 0\}.$$

For our particular case, we have $\psi = \Lambda = \mathbb{1}_{\mathrm{config}_{n,\ell}^{-1}(g_0)}$ and $\Psi = \mathbb{1}_{\{g_0\}}$ and since m is constant and for every $u \in \mathbb{F}_2^\ell$, if $g_0(u) \neq 0$, then $g_0(u) \geqslant \Omega(n)$, it follows that for n sufficiently large, we have $T_m(g_0) = (\mathbb{F}_2^\ell)^m$ and for every $t \in (\mathbb{F}_2^\ell)^m$, $j \in [m]$ and $u \in \mathbb{F}_2^\ell$, we have $(g_0)_{t,j}(u) = g_0(u) + o(n)$. Thus, since $X \in \mathrm{config}_{n,\ell}^{-1}(g_0)$, we have

$$A_v^m \psi(X) = \sum_{t \in (\mathbb{F}_2^\ell)^m} \left(\prod_{j=1}^{m} g_0(t_j) \right) \Psi((g_0)_{t,m}) + o(n^m),$$

where the error term follows since both m and ℓ are constants. Thus, we get

$$A_v^m \Lambda(X) = \sum_{t \in T} \prod_{j=1}^{m} g_0(t_j) + o(n^m),$$

where

$$T \overset{\text{def}}{=} \{t \in (\mathbb{F}_2^\ell)^m \mid (g_0)_{t,m} = g_0\}.$$

For each $t \in T$, let us define a function $F_t \colon \mathbb{F}_2^\ell \to \mathbb{N}$ by $F_t(u) \overset{\text{def}}{=} |t^{-1}(u)|$. Note that we must have $\sum_{u \in \mathbb{F}_2^\ell} F_t(u) = m$ and since $(g_0)_{t,m} = g_0$, we must have

$$\sum_{u \in \mathbb{F}_2^\ell} F_t(u)(\mathbb{1}_{\{v+u\}} - \mathbb{1}_{\{u\}}) = 0,$$

which is equivalent to

$$\forall u \in \mathbb{F}_2^\ell, F_t(u+v) = F_t(u).$$

It is straightforward to check that for $\mathcal{F}_{m,v}$ as in (19), we have $\{F_t \mid t \in T\} = \mathcal{F}_{m,v}$ and that for each $F \in \mathcal{F}_{m,v}$, we have

$$|\{t \in T \mid F_t = F\}| = \binom{m}{F}.$$

Thus, we get

$$A_v^m \Lambda(X) = \sum_{F \in \mathcal{F}_{m,v}} \binom{m}{F} \prod_{u \in \mathbb{F}_2^\ell} g_0(u)^{F(u)} + o(n^m),$$

as desired. ■

6.2 The key functions and matrices

In this section, we provide an abstract way of constructing dual solutions (Theorem 6.7). We refer the reader to Section 3.2 for an informal description.

Given $\ell, n \in \mathbb{N}_+$ and $\varepsilon \in (0,1)$, for every $m \in \mathbb{N}$ and every $u \in \mathbb{F}_2^\ell \setminus \{0\}$, we let

$$\phi_{m,u}(X) \stackrel{\text{def}}{=} \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle u,v \rangle = 1}} \bigl((n - 2|vX|)^m - (\varepsilon n)^m\bigr),$$

$$B_{m,u} \stackrel{\text{def}}{=} \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle u,v \rangle = 1}} (A_v^m - (\varepsilon n)^m I),$$

where $\langle u, v\rangle \stackrel{\text{def}}{=} \sum_{j \in [\ell]} u_j v_j$.

We also define

$$\Phi_m \stackrel{\text{def}}{=} \prod_{u \in \mathbb{F}_2^\ell \setminus \{0\}} \phi_{m,u}, \qquad M_m \stackrel{\text{def}}{=} \prod_{u \in \mathbb{F}_2^\ell \setminus \{0\}} B_{m,u}. \tag{20}$$

Note that these definitions ensure that

$$2^{n\ell} \widehat{\Phi}_m * \Lambda = M_m \Lambda \tag{21}$$

for every $\Lambda \colon \mathbb{F}_2^{\ell \times n} \to \mathbb{R}$.

Lemma 6.5. *For every $u \in \mathbb{F}_2^\ell \setminus \{0\}$, every $X \in \mathrm{Valid}_{n,\ell}^\varepsilon$ and every m even such that*

$$m \geqslant \frac{\ell - 1}{\lg(1/\varepsilon)}, \tag{22}$$

where $\lg \stackrel{\text{def}}{=} \log_2$ is the binary log, the following hold.

i. If there exists $v \in \mathbb{F}_2^\ell$ with $\langle u, v\rangle = 1$ and $vX = 0$, then $\phi_{m,u}(X) \geqslant 0$.

ii. If $vX \neq 0$ for every $v \in \mathbb{F}_2^\ell$ with $\langle u, v \rangle = 1$, then $\phi_{m,u}(X) \leqslant 0$.

iii. If $X \neq 0$, then $\Phi_m(X) \leqslant 0$.

iv. We have

$$\Phi_m(0) = (2^{\ell-1}(1 - \varepsilon^m) n^m)^{2^\ell - 1}.$$

Proof. For Item (i), note that since m is even and $\langle u, v\rangle = 1$, we have

$$\begin{aligned}\phi_{m,u}(X) = \sum_{\substack{v' \in \mathbb{F}_2^\ell \\ \langle u,v' \rangle = 1}} \bigl((n - 2|v'X|)^m - (\varepsilon n)^m\bigr) &\geqslant (n - 2|vX|)^m - 2^{\ell-1} \cdot (\varepsilon n)^m \\ &\geqslant n^m - 2^{\ell-1} \cdot (\varepsilon n)^m \geqslant 0,\end{aligned}$$

where the last inequality follows from (22).

For Item (ii), note that since $X \in \mathrm{Valid}_{n,\ell}^{\varepsilon}$ and

$$\phi_{m,u}(X) = \sum_{\substack{v' \in \mathbb{F}_2^\ell \\ \langle u,v' \rangle = 1}} \big((n - 2|v'X|)^m - (\varepsilon n)^m\big),$$

each $n - 2|v'X|$ in the above is between $-\varepsilon n$ and εn, so since m is even, we get $\phi_{m,u}(X) \leqslant 0$.

For Item (iii), let $V \stackrel{\text{def}}{=} \{v \in \mathbb{F}_2^\ell \mid vX = 0\}$. Clearly V is a linear subspace of $\mathbb{F}_2^\ell$ and since $X \neq 0$, we have $V \neq \mathbb{F}_2^\ell$.

Note now the following chain of equivalences

$$u \in V^\perp \iff \forall v \in \mathbb{F}_2^\ell, (vX = 0 \to \langle v,u \rangle = 0) \iff \forall v \in \mathbb{F}_2^\ell, (\langle v,u \rangle = 1 \to vX \neq 0),$$

so by Item (ii), we get $\phi_{m,u}(X) \leqslant 0$ for every $u \in V^\perp \setminus \{0\}$.

On the other hand, note that if $u \in \mathbb{F}_2^\ell \setminus V^\perp$, then the equivalence above implies that there exists $v \in \mathbb{F}_2^\ell$ with $\langle v,u \rangle = 1$ and $vX = 0$, so Item (i) implies $\phi_{m,u}(X) \geqslant 0$.

Since $V \neq \mathbb{F}_2^\ell$, we have $V^\perp \neq \{0\}$, so $|V^\perp \setminus \{0\}|$ is odd, hence $\Phi_{m,u}(X) \leqslant 0$ as it is a product of an odd number of non-positive factors and some non-negative factors.

Finally, Item (iv) follows by direct calculation. ■

We now compute an alternative formula for M_m.

Lemma 6.6. *We have*

$$M_m = \sum_{\substack{S \subseteq \mathbb{F}_2^\ell \setminus \{0\} \\ |S| \text{ odd}}} \sum_{i \in S} \left(\prod_{u \in S \setminus \{i\}} \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle u,v \rangle = 1}} A_v^m \right) \cdot (\varepsilon n)^{m(2^\ell - 1 - |S|)} \left(\frac{1}{|S|} \cdot \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle i,v \rangle = 1}} A_v^m - \frac{2^{\ell-1} \cdot (\varepsilon n)^m}{2^\ell - |S|} \right). \quad (23)$$

Proof. Let

$$V \stackrel{\text{def}}{=} \{v \colon \mathbb{F}_2^\ell \setminus \{0\} \to \mathbb{F}_2^\ell \mid \forall u \in \mathbb{F}_2^\ell \setminus \{0\}, \langle u, v(u) \rangle = 1\},$$

$$M_{m,v} \stackrel{\text{def}}{=} \sum_{\substack{S \subseteq \mathbb{F}_2^\ell \setminus \{0\} \\ |S| \text{ odd}}} \sum_{i \in S} \left(\prod_{u \in S \setminus \{i\}} A_{v(u)}^m \right) (\varepsilon n)^{m(2^\ell - 1 - |S|)} \left(\frac{A_{v(i)}^m}{|S|} - \frac{(\varepsilon n)^m}{2^\ell - |S|} \right) \qquad (v \in V).$$

We will first show that $M_m = \sum_{v \in V} M_{m,v}$.

Note that

$$M_m = \prod_{u \in \mathbb{F}_2^\ell \setminus \{0\}} B_{m,u} = \prod_{u \in \mathbb{F}_2^\ell \setminus \{0\}} \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle u,v \rangle = 1}} (A_v^m - (\varepsilon n)^m I) = \sum_{v \in V} \prod_{u \in \mathbb{F}_2^\ell \setminus \{0\}} (A_{v(u)}^m - (\varepsilon n)^m I).$$

Our objective is then to show that the inner product in the above is equal to $M_{m,v}$. To prove this, note that

$$\prod_{u \in \mathbb{F}_2^\ell \setminus \{0\}} (A_{v(u)}^m - (\varepsilon n)^m I) = \sum_{S \subseteq \mathbb{F}_2^\ell \setminus \{0\}} \left(\prod_{u \in S} A_{v(u)}^m \right) (-(\varepsilon n)^m)^{2^\ell - 1 - |S|}.$$

We now group the terms in the sum above as follows: we sum over only $S \subseteq \mathbb{F}_2^\ell \setminus \{0\}$ such that $|S|$ is odd and we redistribute the terms with $|S|$ even equally among $S \cup \{i\}$ where i ranges in $\mathbb{F}_2^\ell \setminus (\{0\} \cup S)$. With this redistribution, we have

$$\begin{aligned}
&\prod_{u\in\mathbb{F}_2^\ell\setminus\{0\}} (A^m_{v(u)} - (\varepsilon n)^m I)\\
&= \sum_{\substack{S\subseteq\mathbb{F}_2^\ell\setminus\{0\}\\ |S| \text{ odd}}} \left(\left(\prod_{u\in S} A^m_{v(u)}\right)(-(\varepsilon n))^{m(2^\ell-1-|S|)} + \sum_{i\in S}\frac{1}{2^\ell-|S|}\left(\prod_{u\in S\setminus\{i\}} A^m_{v(u)}\right)(-(\varepsilon n)^m)^{2^\ell-|S|}\right)\\
&= \sum_{\substack{S\subseteq\mathbb{F}_2^\ell\setminus\{0\}\\ |S| \text{ odd}}} \sum_{i\in S} \left(\prod_{u\in S\setminus\{i\}} A^m_{v(u)}\right)(\varepsilon n)^{m(2^\ell-1-|S|)}\left(\frac{A^m_{v(i)}}{|S|} - \frac{(\varepsilon n)^m}{2^\ell-|S|}\right)\\
&= M_{m,v},
\end{aligned}$$

so we conclude that $M_m = \sum_{v\in V} M_{m,v}$.

Finally, note that

$$\begin{aligned}
M_m &= \sum_{v\in V} M_{m,v}\\
&= \sum_{v\in V}\sum_{\substack{S\subseteq\mathbb{F}_2^\ell\setminus\{0\}\\ |S| \text{ odd}}} \sum_{i\in S} \left(\prod_{u\in S\setminus\{i\}} A^m_{v(u)}\right)(\varepsilon n)^{m(2^\ell-1-|S|)}\left(\frac{A^m_{v(i)}}{|S|} - \frac{(\varepsilon n)^m}{2^\ell-|S|}\right)\\
&= \sum_{\substack{S\subseteq\mathbb{F}_2^\ell\setminus\{0\}\\ |S| \text{ odd}}} \sum_{i\in S} \left(\prod_{u\in S\setminus\{i\}} \sum_{\substack{v\in\mathbb{F}_2^\ell\\ \langle u,v\rangle=1}} A^m_{v}\right)\cdot(\varepsilon n)^{m(2^\ell-1-|S|)} \sum_{\substack{v\in\mathbb{F}_2^\ell\\ \langle i,v\rangle=1}} \left(\frac{A^m_{v}}{|S|} - \frac{(\varepsilon n)^m}{2^\ell-|S|}\right)\\
&= \sum_{\substack{S\subseteq\mathbb{F}_2^\ell\setminus\{0\}\\ |S| \text{ odd}}} \sum_{i\in S} \left(\prod_{u\in S\setminus\{i\}} \sum_{\substack{v\in\mathbb{F}_2^\ell\\ \langle u,v\rangle=1}} A^m_{v}\right)\cdot(\varepsilon n)^{m(2^\ell-1-|S|)} \left(\frac{1}{|S|}\cdot\sum_{\substack{v\in\mathbb{F}_2^\ell\\ \langle i,v\rangle=1}} A^m_{v} - \frac{2^{\ell-1}\cdot(\varepsilon n)^m}{2^\ell-|S|}\right),
\end{aligned}$$

so (23) follows. ■

Theorem 6.7. *Let $\ell, m \in \mathbb{N}_+$ with m even such that*

$$m \geqslant \frac{\ell-1}{\lg(1/\varepsilon)}, \tag{24}$$

where $\lg \overset{def}{=} \log_2$ is the binary log.

Suppose further $G \in \mathrm{NConfig}_\ell$ is such that $G(u) > 0$ for every $u \in \mathbb{F}_2^\ell$.

Let further $n \in \mathbb{N}_+$ and suppose that $n\cdot G(u) \in \mathbb{N}$ for every $u \in \mathbb{F}_2^\ell$ and that for $\Lambda \overset{def}{=} \mathbb{1}_{\mathrm{config}^{-1}_{n,\ell}(n\cdot G)}$ and every $i \in \mathbb{F}_2^\ell \setminus \{0\}$, there exists $v \in \mathbb{F}_2^\ell$ with $\langle i, v\rangle = 1$ and

$$A^m_v \Lambda \geqslant (2^{2\ell-1}\varepsilon^m n^m + 1)\Lambda. \tag{25}$$

Finally, let

$$F \stackrel{\text{def}}{=} \Phi_m \cdot \widehat{\Lambda}^2, \qquad\qquad f \stackrel{\text{def}}{=} \frac{F}{\widehat{F}(0)},$$

where Φ_m *is given by* (20).

Then f *is a feasible solution of* (2) *with*

$$\frac{\lg f(0)}{n} \leqslant H_2(G) + O\left(\frac{\lg(n)}{n}\right) \tag{26}$$

as $n \to \infty$ *with* ℓ *fixed.*

Proof. It is clear that $\widehat{f}(0) = 1$.

On the other hand, if $X \in \mathrm{Valid}^{\varepsilon}_{n,\ell} \setminus \{0\}$, then by Lemma 6.5, we have $\Phi_m(X) \leqslant 0$, so we get $f(X) \leqslant 0$.

For the Fourier constraints, by (21), we have

$$\widehat{f} = \frac{\widehat{\Phi_m} * \Lambda * \Lambda}{\widehat{F}(0)} = \frac{M_m \Lambda * \Lambda}{2^{n\ell}\widehat{F}(0)}.$$

Since $\Lambda \geqslant 0$, to show that $\widehat{f} \geqslant 0$, it suffices to show that $M_m\Lambda \geqslant 0$.

By Lemma 6.6, we have

$$M_m = \sum_{\substack{S \subseteq \mathbb{F}_2^\ell \setminus \{0\} \\ |S| \text{ odd}}} \sum_{i \in S} \left(\prod_{u \in S \setminus \{i\}} \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle u,v \rangle = 1}} A_v^m \right) \cdot (\varepsilon n)^{m(2^\ell - 1 - |S|)} \left(\frac{1}{|S|} \cdot \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle i,v \rangle = 1}} A_v^m - \frac{2^{\ell-1} \cdot (\varepsilon n)^m}{2^\ell - |S|} \right)$$

and from the factoring above, it suffices to show that for every $S \subseteq \mathbb{F}_2^\ell \setminus \{0\}$ with $|S|$ odd and every $i \in S$, we have

$$\frac{1}{|S|} \cdot \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle i,v \rangle = 1}} A_v^m \Lambda \geqslant \frac{2^{\ell-1} \cdot (\varepsilon n)^m}{2^\ell - |S|} \Lambda.$$

Since $1 \leqslant |S| \leqslant 2^\ell - 1$, it suffices to then show that

$$\frac{1}{2^\ell} \cdot \sum_{\substack{v \in \mathbb{F}_2^\ell \\ \langle i,v \rangle = 1}} A_v^m \Lambda \geqslant 2^{\ell-1} \cdot (\varepsilon n)^m \Lambda,$$

which follows directly from our assumption (25) (and the fact that all entries of A_v^m and Λ are non-negative). Note that since we have an extra 1 in (25), the argument above in fact implies

$$M_m \Lambda \geqslant \mathrm{poly}(n) \Lambda. \tag{27}$$

It remains to show (26). By Lemma 6.1 and Item (iv), we have

$$F(0) = \Phi_m(0) \cdot \widehat{\Lambda}(0)^2 = (2^{\ell-1}(1-\varepsilon^m)n^m)^{2^\ell-1} \cdot \left(\frac{|\mathrm{config}_{n,\ell}^{-1}(n \cdot G)|}{2^{n\ell}}\right)^2 = \mathrm{poly}(n) \cdot 2^{2(H_2(G)-\ell)n}.$$

On the other hand, we have

$$\widehat{F}(0) = (\widehat{\Phi_m} * \Lambda * \Lambda)(0) = \frac{(M_m\Lambda * \Lambda)(0)}{2^{n\ell}} \geqslant \frac{\mathrm{poly}(n)}{2^{n\ell}}(\Lambda * \Lambda)(0) = \mathrm{poly}(n) \cdot 2^{(H_2(G)-2\ell)n},$$

where the inequality follows from (27) and the last equality follows from Lemma 6.1. Thus, we get

$$\frac{\lg(f(0))}{n} \leqslant H_2(G) + O\left(\frac{\lg(n)}{n}\right),$$

as desired. ■

6.3 Finding Good Configurations

Theorem 6.7 leaves open only one question: which normalized configurations G are such that the corresponding function Λ satisfies (25) while having small binary entropy $H_2(G)$ so as to yield a good value to (2)? In this section, we will see that two kinds of normalized configurations can attain same rates as MRRW (see (15)) up to lower order terms via Theorem 6.7.

Definition 6.8. *Given $\ell \in \mathbb{N}_+$ and $\tau \in [0, 1/\ell]$, the τ-vertex uniform normalized configuration (at level ℓ) is defined as $G_{\tau\text{-vertex-unif}} \in \mathrm{NConfig}_\ell$ given by*

$$G_{\tau\text{-vertex-unif}}(u) \stackrel{\text{def}}{=} \begin{cases} (1-\ell\tau), & \text{if } u = 0, \\ \tau, & \text{if } |u| = 1, \\ 0, & \text{otherwise.} \end{cases}$$

Given $\tau \in [0, 1]$, the τ-quasirandom normalized configuration (at level ℓ) is defined as $G_{\tau\text{-QR}} \in \mathrm{NConfig}_\ell$ given by

$$G_{\tau\text{-QR}}(u) \stackrel{\text{def}}{=} \tau^{|u|}(1-\tau)^{\ell-|u|}.$$

Given further $n \in \mathbb{N}_+$, we let $g_{\tau\text{-vertex-unif}}, g_{\tau\text{-QR}}$ be obtained by rounding $n \cdot G_{\tau\text{-vertex-unif}}$ and $n \cdot G_{\tau\text{-QR}}$ respectively to integer values so that the result is in $\mathrm{Config}_{n,\ell}$.

Lemma 6.9. *Let $\varepsilon \in (0, 1)$, let $\ell \in \mathbb{N}_+$, let $\tau \in (0, 1/\ell)$, let $n, m \in \mathbb{N}_+$ with m even and let $\Lambda \stackrel{\text{def}}{=} \mathbb{1}_{\mathrm{config}_{n,\ell}^{-1}(g_{\tau\text{-vertex-unif}})}$. Then the following hold:*

i. For every $v \in \mathbb{F}_2^\ell$ with $|v| = 1$ and every $X \in \mathrm{config}_{n,\ell}^{-1}(g_{\tau\text{-vertex-unif}})$, we have

$$A_v^m\Lambda(X) = \binom{m}{m/2}(1-\ell\tau)^{m/2}\tau^{m/2}n^m + o(n^m).$$

ii. We have

$$H_2(G_{\tau\text{-vertex-unif}}) = \ell\left(\tau \lg\frac{1}{\tau} + (1-\ell\tau)\lg\frac{1}{1-\ell\tau}\right) = \ell\tau\lg(\tau) + \ell\tau + O(\tau^2),$$

as $\tau \to 0$ with ℓ fixed.

iii. If

$$\tau = \frac{1 - \sqrt{1 - \ell 2^{(4\ell-1)/m} m^{1/m} \varepsilon^2}}{2\ell}, \tag{28}$$

then

$$\tau = \frac{2^{(4\ell-1)/m} m^{1/m}}{4} \varepsilon^2 + O(\varepsilon^4) \tag{29}$$

as $\varepsilon \to 0$ with ℓ and m fixed and

$$A_v^m \Lambda \geqslant 2^{2\ell-1} \varepsilon^m n^m \Lambda + o(n^m) \tag{30}$$

for every $v \in \mathbb{F}_2^\ell$ with $|v| = 1$ as $n \to \infty$ with ε, ℓ and m fixed.

Proof. First note that since $0 < \tau < 1/\ell$, it follows that for every $u \in \mathbb{F}_2^\ell$, if $g_{\tau\text{-vertex-unif}}(u) \neq 0$, then $g_{\tau\text{-vertex-unif}}(u) \geqslant \Omega(n)$, so by Lemma 6.4 with $g_0 \overset{\text{def}}{=} g_{\tau\text{-vertex-unif}}$, we have

$$A_v^m \Lambda(X) = \sum_{F \in \mathcal{F}_{m,v}} \binom{m}{F} \prod_{u \in \mathbb{F}_2^\ell} g_{\tau\text{-vertex-unif}}(u)^{F(u)} + o(n^m),$$

where $\mathcal{F}_{m,v}$ is given by (19).

Since $g_{\tau\text{-vertex-unif}}(u) = 0$ whenever $|u| \geqslant 2$, it follows that the only terms of the sum above that are non-zero correspond to $F \in \mathcal{F}_{m,v}$ that are entirely supported on $\{u \in \mathbb{F}_2^\ell \mid |u| \leqslant 1\}$. Since all $F \in \mathcal{F}_{m,v}$ further satisfy $F(u) = F(u+v)$ for every $u \in \mathbb{F}_2^\ell$, we conclude that only one term of the sum above can be non-zero, namely the one corresponding to $F_0 \in \mathcal{F}_{m,v}$ given by

$$F_0(u) \overset{\text{def}}{=} \begin{cases} \dfrac{m}{2}, & \text{if } u = 0 \text{ or } u = v, \\ 0, & \text{otherwise,} \end{cases}$$

so we get

$$A_v^m \Lambda(X) = \binom{m}{m/2} (1 - \ell\tau)^{m/2} \tau^{m/2} n^m + o(n^m),$$

so Item (i) holds.

For Item (ii), note that

$$\begin{aligned} H_2(G_{\tau\text{-vertex-unif}}) &= \sum_{u \in \mathbb{F}_2^\ell} G_{\tau\text{-vertex-unif}}(u) \lg \frac{1}{G_{\tau\text{-vertex-unif}}(u)} = \ell\tau \lg \frac{1}{\tau} + (1 - \ell\tau) \lg \frac{1}{1 - \ell\tau} \\ &= \ell\tau \lg \frac{1}{\tau} + (1 - \ell\tau)(\ell\tau + O(\tau^2)) = \ell\tau \lg \frac{1}{\tau} + \ell\tau + O(\tau^2). \end{aligned}$$

For Item (iii), first note that (29) follows from (28) and the fact that $\sqrt{1+t} = 1 + t/2 + O(t^2)$ as $t \to 0$.

Finally, note that (30) is trivial when evaluated on a point X not in the support of Λ as the left-hand side is clearly non-negative.

On the other hand, for $X \in \operatorname{supp}(\Lambda)$, that is, for $X \in \operatorname{config}_{n,\ell}^{-1}(g_{\tau\text{-vertex-unif}})$, by Item (i), we have

$$\begin{aligned}
A_v^m \Lambda(X) &= \binom{m}{m/2}(1-\ell\tau)^{m/2}\tau^{m/2}n^m + o(n^m) \\
&\geqslant \frac{2^m}{\sqrt{2m}} \cdot \left(\frac{1-(1-\ell 2^{(4\ell-1)/m}m^{1/m}\varepsilon^2)}{4\ell}\right)^{m/2} + o(n^m) \\
&= 2^{2\ell-1}\varepsilon^m + o(n^m),
\end{aligned}$$

as desired. ■

Lemma 6.10. *Let $\varepsilon \in (0,1)$, let $\ell \in \mathbb{N}_+$, let $\tau \in (0,1)$, let $n, m \in \mathbb{N}_+$ with m even and let $\Lambda \overset{\text{def}}{=} \mathbb{1}_{\operatorname{config}_{n,\ell}^{-1}(g_{\tau\text{-QR}})}$. Then the following hold:*

i. For every $v \in \mathbb{F}_2^\ell$ with $|v| = 1$ and every $X \in \operatorname{config}_{n,\ell}^{-1}(g_{\tau\text{-QR}})$, we have

$$A_v^m \Lambda(X) = \binom{m}{m/2}\tau^{m/2}(1-\tau)^{\ell m/2}(1-2\tau+2\tau^2)^{(\ell-1)m/2}n^m + o(n^m).$$

ii. We have

$$H_2(G_{\tau\text{-QR}}) = \ell\left(\tau \lg\frac{1}{\tau} + (1-\tau)\lg\frac{1}{1-\tau}\right) = \ell\tau\lg\frac{1}{\tau} + \ell\tau + O(\tau^2),$$

as $\tau \to 0$ with ℓ fixed.

iii. If τ is the first non-negative root of

$$4\tau(1-\tau)^\ell(1-2\tau+2\tau^2)^{\ell-1} - 2^{(4\ell-1)/m}m^{1/m}\varepsilon^2 \tag{31}$$

then

$$\tau = \frac{2^{(4\ell-1)/m}m^{1/m}}{4}\varepsilon^2 + O(\varepsilon^{2(1+\ell)}) \tag{32}$$

as $\varepsilon \to 0$ with ℓ and m fixed and

$$A_v^m \Lambda \geqslant 2^{2\ell-1}\varepsilon^m n^m \Lambda + o(n^m) \tag{33}$$

for every $v \in \mathbb{F}_2^\ell$ with $|v| = 1$ as $n \to \infty$ with ε, ℓ and m fixed.

Proof. First note that since $0 < \tau < 1$, it follows that $g_{\tau\text{-QR}}(u) \geqslant \Omega(n)$ for every $u \in \mathbb{F}_2^\ell$, so by Lemma 6.4 with $g_0 \overset{\text{def}}{=} g_{\tau\text{-QR}}$, we have

$$A_v^m \Lambda(X) = \sum_{F \in \mathcal{F}_{m,v}} \binom{m}{F} \prod_{u \in \mathbb{F}_2^\ell} g_{\tau\text{-QR}}(u)^{F(u)} + o(n^m),$$

where $\mathcal{F}_{m,v}$ is given by (19).

Let $i_0 \in \operatorname{supp}(v)$ and note that there is a natural one-to-one correspondence between $\mathcal{F}_{m,v}$ and the set

$$\mathcal{F} \overset{\text{def}}{=} \left\{ F\colon \mathbb{F}_2^{[\ell]\setminus\{i_0\}} \to \mathbb{N} \;\middle|\; \sum_{u\in\mathbb{F}_2^{[\ell]\setminus\{i_0\}}} F(u) = \frac{m}{2} \right\}$$

in which $F \in \mathcal{F}_{m,v}$ corresponds to $F|_{\mathbb{F}_2^{[\ell]\setminus\{i_0\}}}$. Thus, we get

$$\begin{aligned}
A_v^m \Lambda(X) &= \sum_{F\in\mathcal{F}} \binom{m}{F, F} \prod_{u\in\mathbb{F}_2^{[\ell]\setminus\{i_0\}}} (g_{\tau\text{-QR}}(u) g_{\tau\text{-QR}}(u+v))^{F(u)} + o(n^m) \\
&= \binom{m}{m/2} \sum_{F\in\mathcal{F}} \binom{m/2}{F}^2 \prod_{u\in\mathbb{F}_2^{[\ell]\setminus\{i_0\}}} (\tau^{2|u|+1}(1-\tau)^{2\ell-2|u|-1})^{F(u)} n^m + o(n^m) \\
&\geqslant \binom{m}{m/2} \sum_{F\in\mathcal{F}} \binom{m/2}{F} \prod_{u\in\mathbb{F}_2^{[\ell]\setminus\{i_0\}}} (\tau^{2|u|+1}(1-\tau)^{2\ell-2|u|-1})^{F(u)} n^m + o(n^m) \\
&= \binom{m}{m/2} \left(\sum_{u\in\mathbb{F}_2^{[\ell]\setminus\{i_0\}}} \tau^{2|u|+1}(1-\tau)^{2\ell-2|u|-1} \right)^{m/2} n^m + o(n^m) \\
&= \binom{m}{m/2} \tau^{m/2}(1-\tau)^{(2\ell-1)m/2} \left(1 + \left(\frac{\tau}{1-\tau}\right)^2 \right)^{(\ell-1)m/2} n^m + o(n^m) \\
&= \binom{m}{m/2} \tau^{m/2}(1-\tau)^{\ell m/2}(1-2\tau+2\tau^2)^{(\ell-1)m/2} n^m + o(n^m),
\end{aligned}$$

where the third equality follows from the Multinomial Theorem and the fourth equality follows from the Binomial Theorem. Thus, Item (i) holds.

For Item (ii), note that

$$\begin{aligned}
H_2(G_{\tau\text{-QR}}) &= \sum_{u\in\mathbb{F}_2^\ell} \tau^{|u|}(1-\tau)^{\ell-|u|} \lg \frac{1}{\tau^{|u|}(1-\tau)^{\ell-|u|}} \\
&= \sum_{j=0}^{\ell} \binom{\ell}{j} \tau^j (1-\tau)^{\ell-j} \left(j \cdot \lg\frac{1}{\tau} + (\ell-j) \lg \frac{1}{1-\tau} \right) \\
&= \ell \left(\tau \lg \frac{1}{\tau} + (1-\tau) \lg \frac{1}{1-\tau} \right) \\
&= \ell\tau \lg \frac{1}{\tau} + \ell\tau + O(\tau^2).
\end{aligned}$$

For Item (iii), first note that the expression in (31) takes a negative value when $\tau = 0$ and takes the value

$$2^{3-2\ell} - 2^{(4\ell-1)/m} m^{1/m} \varepsilon^2$$

when $\tau = 1/2$, which is positive if $\varepsilon > 0$ is small enough, so the expression in (31) has a non-negative root before 1/2. If τ is the first non-negative root in (31), then (32) follows straightforwardly.

Finally, note that (33) is trivial when evaluated on a point X not in the support of Λ as the left-hand side is clearly non-negative.

On the other hand, for $X \in \operatorname{supp}(\Lambda)$, that is, for $X \in (\operatorname{config}^v_{n,\ell})^{-1}(g_{\tau\text{-QR}})$, by Item (i), we have

$$\begin{aligned} A^m_v \Lambda(X) &= \binom{m}{m/2} \tau^{m/2}(1-\tau)^{\ell m/2}(1-2\tau+2\tau^2)^{(\ell-1)m/2} n^m + o(n^m) \\ &\geqslant \frac{2^m}{\sqrt{2m}} \tau^{m/2}(1-\tau)^{\ell m/2}(1-2\tau+2\tau^2)^{(\ell-1)m/2} n^m + o(n^m) \\ &= 2^{2\ell-1} m^{1/m} \varepsilon^m n^m + o(n^m), \end{aligned}$$

where the second equality follows since τ is a root of (31). ■

Corollary 6.11. *Let $\varepsilon \in (0,1)$, let $\ell, m \in \mathbb{N}_+$ with m even such that*

$$m \geqslant \frac{\ell - 1}{\lg(1/\varepsilon)},$$

where $\lg \overset{\text{def}}{=} \log_2$ is the binary log.

Then for every sufficiently large n, there exist $g_1, g_2 \in \operatorname{Config}_{n,\ell}$ with

$$|g_1(u) - n \cdot G_{\tau\text{-vertex-unif}}(u)| \leqslant o(n), \qquad |g_2(u) - n \cdot G_{\tau\text{-QR}}(u)| \leqslant o(n)$$

for every $u \in \mathbb{F}_2^\ell$ such that for

$$\Lambda_i \overset{\text{def}}{=} \mathbb{1}_{\operatorname{config}^{-1}_{n,\ell}(g_i)}, \qquad F_i \overset{\text{def}}{=} \Phi_m \cdot \widehat{\Lambda}_i^2, \qquad f_i \overset{\text{def}}{=} \frac{F_i}{\widehat{F_i}(0)},$$

where Φ_m is given by (20), we have that f_1 and f_2 are feasible solutions of (2) with

$$\begin{aligned} \frac{\lg f_i(0)}{n} &\leqslant \frac{2^{(4\ell-1)/m} m^{1/m}}{4} \varepsilon^2 \lg \frac{1}{\varepsilon} + O(\varepsilon^4) + O_\varepsilon\left(\frac{\lg(n)}{n}\right) \\ &= \frac{1+o(1)}{4} \varepsilon^2 \lg \frac{1}{\varepsilon} + O_\varepsilon\left(\frac{\lg(n)}{n}\right) \end{aligned}$$

as $n \to \infty$ and $\varepsilon \to 0$ with ℓ and m fixed (in the above, the error term $O_\varepsilon(\lg(n)/n)$ hides multiplicative factors dependent on ε, but the error terms $o(1)$ and $O(\varepsilon^4)$ only hide multiplicative factors that do not depend on n nor on ε).

Proof. Follows by combining Lemmas 6.9 and 6.10 with Theorem 6.7 (note that the small adjustment to the configurations is needed both due to the error terms in (30) and (33) and to obtain the extra 1 term needed in (25)). ■

7 Conclusion

Establishing tight bounds on the rate-vs-distance trade-off of binary codes has remained a major open question in coding theory. The best existential constructions given by the Gilbert–Varshamov bound have not been improved for over 70 years, and the best upper bounds given by MRRW bound have not been improved for almost 50 years. These known bounds are the same even for the important class of linear codes. With the inception of complete linear programming hierarchies for linear codes extending Delsarte's LPs, an ambitious research program of analyzing these higher-order Delsarte LPs is launched. On one hand their similarity with the original Delsarte LPs gives hope this might be a viable task. On the other hand, the higher-order structure poses non-trivial challenges.

We view the contributions of this work as establishing important milestones in this research program as we are able to construct higher-order dual feasible solutions for the first time. This is done in two complementary ways. First, by explicitly lifting dual solutions from lower levels to higher levels of these hierarchies. Second, by constructing higher-order dual solutions from scratch generalizing spectral-based techniques. Given that these constructions either match or approximately match the best known bounds, together with the proven strength of these complete hierarchies, they open up important avenues of further exploration. For instance, very interesting concrete questions made possible by this work are the following.

- After lifting a dual solution of the original Delsate LP to a higher-level ℓ of these hierarchies, can we improve its objective value and improve over the MRRW bound?
- We saw that the spectral-based construction has some degrees of freedom, namely, there is a choice of function ϕ capturing the sign of the valid region and a choice of configurations for an eigenvalue-like problem. Can we find suitable choices to improve the MRRW bound?

Acknowledgments

The authors are very thankful for the support and hospitality of IAS and the Simons Institute. LC, FGJ and EL thank Avi Wigderson for hosting them at the wonderful IAS, where part of this work was done. In particular, we would like to highlight the importance to us of the programs and clusters: "HDX and Codes", "Analysis and TCS: New Frontiers", "Error-Correcting Codes: Theory and Practice", and "Quantum Algorithms, Complexity, and Fault Tolerance". FGJ thanks Venkat Guruswami for kindly hosting him in his fantastic research groups. FGJ thanks the support in part as a Google Research Fellow.

CJ is a member of the Bocconi Institute for Data Science and Analytics (BIDSA). Work supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement Nos. 834861 and 101019547).

References

[Bac06] Christine Bachoc. Linear programming bounds for codes in Grassmannian spaces. *IEEE Trans. Inform. Theory*, 52(5):2111–2125, 2006. doi:10.1109/TIT.2006.872973. 1

[BN06] A. M. Barg and D. Yu. Nogin. Spectral approach to linear programming bounds on codes. *Probl. Inf. Transm.*, 42(2):77–89, apr 2006. doi:10.1134/S0032946006020025. 1, 9

[BN08] Alexander Barg and Dmitry Nogin. A functional view of upper bounds on codes. In *Coding and cryptology*, volume 4 of *Ser. Coding Theory Cryptol.*, pages 15–24. World Sci. Publ., Hackensack, NJ, 2008. URL: https://doi.org/10.1142/9789812832245_0002, doi:10.1142/9789812832245_0002. 1

[BV08] Christine Bachoc and Frank Vallentin. New upper bounds for kissing numbers from semidefinite programming. *J. Amer. Math. Soc.*, 21(3):909–924, 2008. doi:10.1090/S0894-0347-07-00589-9. 1

[CDA24] André Chailloux and Thomas Debris-Alazard. New solutions to delsarte's dual linear programs, 2024. arXiv:2405.07666. 1

[CE03] Henry Cohn and Noam Elkies. New upper bounds on sphere packings. I. *Ann. of Math. (2)*, 157(2):689–714, 2003. doi:10.4007/annals.2003.157.689. 1, 4

[CJJ22] Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones. A complete linear programming hierarchy for linear codes. In *13th Innovations in Theoretical Computer Science Conference*, volume 215 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 51, 22. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2022. 1, 2, 3, 4, 5, 11

[CJJ23] Leonardo Nagami Coregliano, Fernando Granha Jeronimo, and Chris Jones. Exact completeness of LP hierarchies for linear codes. In *14th Innovations in Theoretical Computer Science Conference*, volume 251 of *LIPIcs. Leibniz Int. Proc. Inform.*, pages Art. No. 40, 18. Schloss Dagstuhl. Leibniz-Zent. Inform., Wadern, 2023. doi:10.4230/lipics.itcs.2023.40. 1, 3, 10, 19

[CKM$^+$17] Henry Cohn, Abhinav Kumar, Stephen D. Miller, Danylo Radchenko, and Maryna Viazovska. The sphere packing problem in dimension 24. *Ann. of Math. (2)*, 185(3):1017–1033, 2017. doi:10.4007/annals.2017.185.3.8. 1, 4

[Del73] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973. 1

[FT05] Joel Friedman and Jean-Pierre Tillich. Generalized Alon-Boppana theorems and error-correcting codes. *SIAM J. Discrete Math.*, 19(3):700–718, 2005. doi:10.1137/S0895480102408353. 1

[GMS12] Dion C Gijswijt, Hans D Mittelmann, and Alexander Schrijver. Semidefinite code bounds based on quadruple distances. *IEEE Transactions on Information Theory*, 58(5):2697–2705, 2012. 1

[Gop93] V. D. Goppa. Bounds for codes. *Dokl. Akad. Nauk*, 1993. 1

[JV04] Tao Jiang and A. Vardy. Asymptotic improvement of the gilbert-varshamov bound on the size of binary codes. *IEEE Transactions on Information Theory*, 50(8):1655–1664, 2004. doi:10.1109/TIT.2004.831751. 1

[Las15] Jean Bernard Lasserre. *An introduction to polynomial and semi-algebraic optimization.* Cambridge Texts in Applied Mathematics. Cambridge University Press, Cambridge, 2015. doi:10.1017/CBO9781107447226. 1

[Lau07] Monique Laurent. Strengthened semidefinite programming bounds for codes. *Math. Program.*, 109(2-3):239–261, 2007. doi:10.1007/s10107-006-0030-3. 1

[Lev98] Vladimir I. Levenshtein. Universal bounds for codes and designs. In *Handbook of coding theory, Vol. I, II*, pages 499–648. North-Holland, Amsterdam, 1998. 1

[LL22] Elyassaf Loyfer and Nati Linial. Linear programming hierarchies in coding theory: Dual solutions, 2022. URL: https://arxiv.org/abs/2211.12977, arXiv:2211.12977. 8, 9

[LL23a] Nati Linial and Elyassaf Loyfer. An elementary proof of the first lp bound on the rate of binary codes, 2023. arXiv:2303.16619. 1, 10

[LL23b] Elyassaf Loyfer and Nati Linial. New LP-based upper bounds in the rate-vs.-distance problem for binary linear codes. *IEEE Trans. Inform. Theory*, 69(5):2886–2899, 2023. doi:10.1109/tit.2023.3236660. 1, 4, 5, 6, 10

[MRRW77] Robert J. McEliece, Eugene R. Rodemich, Howard Rumsey, Jr., and Lloyd R. Welch. New upper bounds on the rate of a code via the Delsarte-MacWilliams inequalities. *IEEE Trans. Inform. Theory*, IT-23(2):157–166, 1977. doi:10.1109/tit.1977.1055688. 1, 3, 9

[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. doi:10.1109/SFCS.2005.55. 1, 8, 9

[NS09] Michael Navon and Alex Samorodnitsky. Linear programming bounds for codes via a covering argument. *Discrete Comput. Geom.*, 41(2):199–207, 2009. doi:10.1007/s00454-008-9128-0. 1

[Sam01] Alex Samorodnitsky. On the optimum of Delsarte's linear program. *J. Combin. Theory Ser. A*, 96(2):261–287, 2001. doi:10.1006/jcta.2001.3176. 1

[Sam23a] Alex Samorodnitsky. On the difficulty to beat the first linear programming bound for binary codes, 2023. URL: https://arxiv.org/abs/2308.16038, arXiv:2308.16038. 8

[Sam23b] Alex Samorodnitsky. One more proof of the first linear programming bound for binary codes and two conjectures, 2023. doi:10.1007/s11856-023-2514-8. 1

[Sch05] Alexander Schrijver. New code upper bounds from the Terwilliger algebra and semidefinite programming. *IEEE Trans. Inform. Theory*, 51(8):2859–2866, 2005. doi:10.1109/TIT.2005.851748. 1

[Via17] Maryna S. Viazovska. The sphere packing problem in dimension 8. *Ann. of Math. (2)*, 185(3):991–1015, 2017. doi:10.4007/annals.2017.185.3.7. 1, 4

A Other Formulations of the Hierarchy

In this section we state other formulations that are not used in the current work.

A.1 Lovász ϑ' Formulation

The ϑ' formulation mentioned in Section 2 is (34), whose dual is (35); a linear code $C \in \mathrm{Valid}_n$ yields a natural solution M_C of (34) given by $M_C(X,Y) \overset{\mathrm{def}}{=} \mathbb{1}[X_1,\ldots,X_\ell,Y_1,\ldots,Y_\ell \in C]/|C|^\ell$, whose value is $|C|^\ell$.

$$\boxed{\begin{array}{lll}
\text{Variables: } M\colon \mathbb{F}_q^{\ell\times n}\times\mathbb{F}_q^{\ell\times n}\to\mathbb{R} \text{ symmetric} & & \\
\quad\max & \displaystyle\sum_{X,Y\in\mathbb{F}_q^{\ell\times n}} M(X,Y) & \\
\quad\text{s.t.} & \operatorname{tr}(M)=1 & \text{(Normalization)} \\
 & M(X,Y)=0 \quad \forall X,Y\in\mathbb{F}_q^{\ell\times n} \text{ with } X-Y\notin \mathrm{Valid}_{n,\ell} & \text{(Validity)} \\
 & M\succeq 0 & \text{(Positive semidefiniteness)} \\
 & M(X,Y)\geqslant 0 \quad \forall X,Y\in\mathbb{F}_q^{\ell\times n} & \text{(Non-negativity)}
\end{array}} \tag{34}$$

$$\boxed{\begin{array}{lll}
\text{Variables: } N\colon \mathbb{F}_q^{\ell\times n}\times\mathbb{F}_q^{\ell\times n}\to\mathbb{R} \text{ symmetric} & & \\
\quad\min & \beta & \\
\quad\text{s.t.} & \beta I - N\succeq 0 & \text{(Maximum eigenvalue)} \\
 & N(X,Y)\geqslant 1 \quad \forall X,Y\in\mathbb{F}_q^{\ell\times n} \text{ with } X-Y\in \mathrm{Valid}_{n,\ell} & \text{(Validity)}
\end{array}} \tag{35}$$

A.2 LP Formulation

To get from the ϑ' formulation of (34) to the LP formulation of (1), one first notes that all $\mathbb{F}_q^n$-symmetric solutions must lie in the span of the matrices

$$E_Z(X,Y) \overset{\mathrm{def}}{=} \mathbb{1}[X-Y=Z] \qquad\qquad (X,Y,Z\in\mathbb{F}_q^{\ell\times n}).$$

On the other hand, the space of $\mathbb{F}_q^n$-invariant solutions is the also the span of the Fourier matrices

$$F_Z(X,Y) \overset{\mathrm{def}}{=} \chi_Z(X)\overline{\chi}_Z(Y) \qquad\qquad (X,Y,Z\in\mathbb{F}_q^{\ell\times n}),$$

which are positive semidefinite. The corresponding change of variables is summarized by

$$\sum_{Z\in\mathbb{F}_q^{\ell\times n}} f(Z)E_Z = \sum_{Z\in\mathbb{F}_q^{\ell\times n}} \widehat{f}(Z)F_Z, \qquad \widehat{f}(Z) \overset{\mathrm{def}}{=} \frac{1}{q^{n\ell}}\sum_{X\in\mathbb{F}_q^{\ell\times n}} f(X)\overline{\chi_Z(X)} \qquad (f\in\mathbb{C}^{\mathbb{F}_q^{\ell\times n}}).$$

Since any $\mathbb{F}_q^n$-symmetric solution is of the first form above for some $f\colon\mathbb{F}_q^{\ell\times n}\to\mathbb{C}$, the semidefinite constraint amounts to non-negativity of $\widehat{f}$ and all other constraints translate easily to linear constraints on f.

A.3 Krawtchouk Formulation

The Krawtchouk formulation mentioned in Section 2 uses the S_n-symmetry to rewrite the Fourier transform in terms of the higher-order Krawtchouk polynomials $K_h\colon \mathrm{Config}_{n,\ell} \to \mathbb{C}$ ($h \in \mathrm{Config}_{n,\ell}$) given by

$$K_h(g) \overset{\text{def}}{=} \sum_{F\in\mathcal{F}_{g,h}} \prod_{w\in\mathbb{F}_q^\ell} \binom{g(w)}{F(-,w)} \prod_{u,w\in\mathbb{F}_q^\ell} \chi_u(w)^{F(u,w)},$$

$$\mathcal{F}_{g,h} \overset{\text{def}}{=} \left\{ F\colon \mathbb{F}_q^\ell \times \mathbb{F}_q^\ell \to \mathbb{N} \;\middle|\; \sum_{u\in\mathbb{F}_q^\ell} F(u,-) = g \wedge \sum_{w\in\mathbb{F}_q^\ell} F(-,w) = h \right\},$$

$$\binom{g(w)}{F(-,w)} \overset{\text{def}}{=} \frac{g(w)!}{\prod_{u\in\mathbb{F}_q^\ell} F(u,w)!}, \qquad \chi_u(w) \overset{\text{def}}{=} \exp\left(\frac{2\pi i u w}{q}\right).$$

In both the Krawtchouk formulation of (36) and its dual in (37) below, $g^- \in \mathrm{Config}_{n,\ell}$ denotes the configuration given by $g^-(u) \overset{\text{def}}{=} g(-u)$; a linear code $C \in \mathrm{Valid}_n$ yields a natural solution f_C of (36) given by $f_C(g) \overset{\text{def}}{=} |\{X \in (\mathrm{config}_{n,\ell})^{-1}(g) \mid X_1, \ldots, X_\ell \in C\}|$.

$$\begin{array}{|llll|}\hline
\text{Variables: } f\colon \mathrm{Config}_{n,\ell} \to \mathbb{R} & & & \\
\max & \displaystyle\sum_{g\in\mathrm{Config}_{n,\ell}} f(g) & & \\
\text{s.t.} & f(\mathrm{config}_{n,\ell}(0)) = 1 & & \text{(Normalization)} \\
 & f(g) = 0 & \forall g \in \mathrm{config}_{n,\ell}(\mathbb{F}_q^{\ell\times n} \setminus \mathrm{Valid}_{n,\ell}) & \text{(Validity)} \\
 & \displaystyle\sum_{g\in\mathrm{Config}_{n,\ell}} K_h(g) f(g) \geqslant 0 & \forall h \in \mathrm{Config}_{n,\ell} & \text{(Krawtchouk)} \\
 & f(g) \geqslant 0 & \forall g \in \mathrm{Config}_{n,\ell} & \text{(Non-negativity)} \\
 & f(g) = f(g^-) & \forall g \in \mathrm{Config}_{n,\ell} & \text{(Symmetry)} \\ \hline
\end{array} \tag{36}$$

$$\begin{array}{|llll|}\hline
\text{Variables: } f\colon \mathrm{Config}_{n,\ell} \to \mathbb{R}, \beta\colon \mathrm{Config}_{n,\ell} \to \mathbb{R} & & & \\
\min & 1 + \displaystyle\sum_{g\in\mathrm{Config}_{n,\ell}} K_g(0) f(g) & & \\
\text{s.t.} & 1 + \displaystyle\sum_{g\in\mathrm{Config}_{n,\ell}} K_g(h) f(g) + \beta(g) - \beta(g^-) \leqslant 0 & \forall h \in \mathrm{config}_{n,\ell}(\mathrm{Valid}_{n,\ell} \setminus \{0\}) & \text{(Validity)} \\
 & f(g) \geqslant 0 & \forall g \in \mathrm{Config}_{n,\ell} & \text{(Non-negativity)} \\ \hline
\end{array} \tag{37}$$

An alternative way of obtaining (36) is directly from the Lovász ϑ' formulation (34) by symmetrizing the action of the natural semidirect product $\mathbb{F}_q^n \rtimes S_n$ that joins the actions of $\mathbb{F}_q^n$ and S_n into a single action. In turn, this amounts to the observation that this $\mathbb{F}_q^n \rtimes S_n$-action turns $\mathbb{F}_q^{\ell\times n}$ naturally into a association scheme that is both a translation scheme and Schurian.

B Notation

The set of non-negative integers is denoted by $\mathbb{N}$ and the set of positive integers is denoted by $\mathbb{N}_+ \overset{\text{def}}{=} \mathbb{N} \setminus \{0\}$. For $n \in \mathbb{N}$, we let $[n] \overset{\text{def}}{=} \{1, \ldots, n\}$. We also let $\mathbb{R}_+$ be the set of non-negative reals.

For $q, n \in \mathbb{N}$, we denote the *nth geometric sum of ratio q* by

$$[n]_q \overset{\text{def}}{=} \sum_{j=0}^{n-1} q^j = \begin{cases} \dfrac{q^n - 1}{q - 1}, & \text{if } q \neq 1, \\ n, & \text{if } q = 1. \end{cases}$$

We extend the notation above to when $n \leqslant 0$ in the natural way so that $\sum_{j=a}^{a-1} c_j = 0$ and $\sum_{j=a}^{b} c_j = -\sum_{j=b+1}^{a-1} c_j$.

Given further $k \in \mathbb{Z}$, we denote the *q-Gaussian falling factorial of n by k*, the *q-Gaussian factorial* and the *q-Gaussian binomial of n by k* by

$$(n)_{k,q} \overset{\text{def}}{=} \prod_{j=0}^{k-1} [n-j]_q, \qquad k!_q \overset{\text{def}}{=} (k)_{k,q}, \qquad \binom{n}{k}_q \overset{\text{def}}{=} \begin{cases} \dfrac{(n)_{k,q}}{k!_q}, & \text{if } k \geqslant 0, \\ 0, & \text{otherwise,} \end{cases}$$

respectively. When $k \leqslant 0$, products should be interpreted in the usual fashion so that $\prod_{j=a}^{a-1} c_j = 1$ and $\prod_{j=a}^{b} c_j = \prod_{j=b+1}^{a-1} c_j^{-1}$. We will omit q from the notation when $q = 1$, so that the above match the usual falling factorial, factorial and binomial, respectively.

For a set V and $k \in \mathbb{Z}$, we denote by $\binom{V}{k}$ the set of all subsets of V of size k (so $|\binom{V}{k}| = \binom{|V|}{k}$ when V is finite).

For a prime power $q \in \mathbb{N}$, we denote by $\mathbb{F}_q$ the field with q elements and for $x \in \mathbb{F}_q^n$, we denote by $|x| \overset{\text{def}}{=} |\operatorname{supp}(x)|$ the *Hamming weight* of x. For an $\mathbb{F}_q$-vector space V, we denote by $L_{\mathbb{F}_q}(V)$ the set of all $\mathbb{F}_q$-linear subspaces of V and we denote by $\mathrm{GL}_\ell(\mathbb{F}_q)$ the general linear group of degree ℓ over $\mathbb{F}_q$ (i.e., the group of non-singular $\ell \times \ell$ matrices over $\mathbb{F}_q$). For a matrix X, we denote by X_i the ith row of X and by $X_{i_1,\ldots,i_t}$ the matrix obtained by restricting X to the rows indexed by $i_1, \ldots, i_t$.

A *distance-d code* is a code $C \subseteq \mathbb{F}_q^n$ such that $|x - y| \geqslant d$ for all $x, y \in C$ with $x \neq y$. We denote by $A_q(n, d)$ the size of the largest distance-d code in $\mathbb{F}_q^n$ and by $A_q^{\mathrm{Lin}}(n, d)$ the size of the largest distance-d code in $\mathbb{F}_q^n$ that is also a subspace of $\mathbb{F}_q^n$.