

The asymptotic number of equivalence classes of linear codes with given dimension

Andrea Di Giusto*, and Alberto Ravagnani†

Eindhoven University of Technology, the Netherlands

Abstract

We investigate the asymptotic number of equivalence classes of linear codes with prescribed length and dimension. While the total number of inequivalent codes of a given length has been studied previously, the case where the dimension varies as a function of the length has not yet been considered. We derive explicit asymptotic formulas for the number of equivalence classes under three standard notions of equivalence, for a fixed alphabet size and increasing length. Our approach also yields an exact asymptotic expression for the sum of all q -binomial coefficients, which is of independent interest and answers an open question in this context. Finally, we establish a natural connection between these asymptotic quantities and certain discrete Gaussian distributions arising from Brownian motion, providing a probabilistic interpretation of our results.

1 Introduction

Studying error-correcting codes up to equivalence is a well-established practice in coding theory. Equivalent codes share all the properties that are relevant for a particular application, and can *de facto* be used interchangeably. When focusing on linear block codes endowed with the Hamming metric, there exist three main notions of equivalence, each corresponding to a group action: *permutation* equivalence, *monomial* equivalence (probably the most popular), and *semilinear* equivalence. For binary block codes, these three notions coincide.

A natural question in coding theory is to count the number of q -ary codes that satisfy a particular property. When such property is having given *length* n , *dimension* k , and *minimum distance* at least d , the problem is equivalent to computing the parameters of certain lattices that are notoriously difficult to analyse [5, 2, 3, 16]. When working modulo code equivalence, one natural question is to compute the number of equivalence classes of q -ary codes with given length n and dimension k , which is yet another impossible task. This paper addresses the asymptotic version of this problem, solving it entirely for some parameters ranges.

*A.D.G. is supported by the European Commission through MSCA-DN project ENCODE.

†A.R. is supported by the Dutch Research Council NWO through grants OCENW.KLEIN.539 and VI.Vidi.203.045, by the European Commission via the ENCODE MSCA-DN project, by the EuroTech Alliance, and by the Royal Academy of Arts and Sciences of the Netherlands.

The problem of counting codes up to equivalence has been considered before in the coding theory literature. However, all references we are aware of focus on estimating the number of equivalence classes of codes over a given alphabet and with given length, *without* fixing the code dimension. This paper fills in this gap by estimating the number of equivalence classes of codes whose dimension is k , and where $k = k(n)$ is a function of the length n . One of our main results determines the exact asymptotic behaviour of the number of equivalence classes for q fixed and n growing. More precisely, in Theorem 4.1 we show that, for sufficiently well-behaved dimension functions $k(n)$, the asymptotic numbers of permutation, monomial, and semilinear equivalence classes are

$$\frac{q^{k(n)(n-k(n))}}{K_q n!}, \quad \frac{q^{k(n)(n-k(n))}}{K_q n! (q-1)^{n-1}}, \quad \frac{q^{k(n)(n-k(n))}}{K_q h n! (q-1)^{n-1}},$$

respectively. We then relate these quantities to the (better studied) number of equivalence classes of codes with unrestricted dimension. Interestingly, for a suitable choice of $k(n)$ the relation can be expressed very naturally using the Gaussian θ_2 and θ_3 distributions, which control the dynamics of the Brownian motion.

Our results are not necessarily related to the theory of error-correcting codes, and include asymptotic estimates of quantities that are of interest also in other fields, such as the q -binomial coefficients. As a byproduct of our analysis, we also determine the exact asymptotic behaviour of the sum of all q -binomials for fixed q and $n \rightarrow \infty$, answering an open question raised by Wild in [18].

Before presenting the structure of the paper, we briefly survey the contributions to the problem made so far and introduce the various players. The study of the asymptotic number of monomially inequivalent binary codes was initiated by Wild in [18]. His main statement was correct, but a gap in the proof was found by Lax in [15]. A correct proof was later published by Hou in [10]. The state-of-the-art reference on monomial and permutation equivalence classes of q -ary linear codes is [9], where Hou shows that the number $\mathcal{N}_n$ of monomially inequivalent q -ary linear codes of length n satisfies

$$\mathcal{N}_n \sim \frac{\sum_{j=0}^n \binom{n}{j}_q}{n! (q-1)^{n-1}} \quad \text{for } n \text{ large.} \quad (1)$$

However, the paper does not address the case where the dimension is restricted to a specific function $k(n)$ of the length. For semilinear classes and a sum-up of the three notions of equivalence, see [11], also by Hou. The focus of this paper is the quantity $\mathcal{N}_{k,n}$, counting the number of inequivalent codes of a given dimension $k = k(n)$.

Outline. The remainder of this paper is organized as follows. In Section 2 we establish the necessary background and formally state the problem studied in this paper. In Section 3 we show the asymptotic relation between the number of inequivalent codes and q -binomial coefficients; in particular, we outline the limitations needed on the function $k(n)$ describing the dimension of the equivalence classes. Section 4 is devoted to the study of the q -binomial coefficient $\binom{n}{k(n)}_q$ as n grows, and consequently to the description of the asymptotic number of inequivalent codes of dimension $k(n)$. We then turn to the study of the proportion between this number and the number of all equivalence classes (without restriction on the dimension) in Section 5. We explain the link between these numbers and the Gaussian θ_2 and θ_3 distributions, and offer an asymptotic description of the sum of all q -binomials.

2 Preliminaries and problem statement

We start by establishing the notation for this paper and by stating the problem we are interested in. In the sequel, the closed interval with extrema $a, b \in \mathbb{R}$ is denoted by $[a, b]$; for $b \geq 1$, we let $[b] = [1, b]$. For $x \in \mathbb{R}$, $\lfloor x \rfloor$ (resp. $\lceil x \rceil$) is the greatest (resp. smallest) $z \in \mathbb{Z}$ such that $z \leq x$ ($z \geq x$). Throughout the paper we follow Bachmann-Landau notation notation ($\sim$, O , o) for asymptotic estimates; see [4]. All asymptotics are for $n \rightarrow \infty$, unless otherwise specified.

We include the coding theory background needed to read this paper; we refer to [12] for further details. With q we always denote a prime power, $\mathbb{F}_q$ is the field with q elements, and we let $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. We often omit q from the notations: the reader can assume it is fixed, unless otherwise specified.

Definition 2.1. A **(linear) code** is a vector subspace $\mathcal{C}$ of $\mathbb{F}_q^n$. The **dimension** of $\mathcal{C}$ is its dimension over $\mathbb{F}_q$ as a linear space. The **Hamming weight** of a vector $x = (x_1, \dots, x_n) \in \mathbb{F}_q^n$ is the number of its nonzero coordinates: $w(x) = |\{i \in [n] \mid x_i \neq 0\}|$. The **(Hamming) distance** between $x, y \in \mathbb{F}_q^n$ is the Hamming weight of their difference: $d(x, y) = w(x - y)$.

The above notions are central in characterizing the error correcting capabilities of a code: the **minimum distance** of a nonzero code $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{d(c_1, c_2) \mid c_1, c_2 \in \mathcal{C}, c_1 \neq c_2\} = \min\{w(c) \mid c \in \mathcal{C}, c \neq 0\},$$

and the maximum amount of errors that a code $\mathcal{C}$ can correct is $\lfloor (d(\mathcal{C}) - 1)/2 \rfloor$.

For $0 \leq k \leq n$, the **Grassmannian** $\mathcal{G}(k, n)$ is the set of all codes of dimension k in $\mathbb{F}_q^n$; its cardinality is the q -binomial coefficient n -choose- k . The **projective space** is the union of all Grassmannians $\mathcal{G}(n) = \cup_{k=0}^n \mathcal{G}(k, n)$; its cardinality, which is the sum of $|\mathcal{G}(k, n)|$ for k from 0 to n , is denoted by $S(n)$. In formulæ, we have

$$|\mathcal{G}(k, n)| = \binom{n}{k}_q = \prod_{j=0}^{k-1} \frac{q^{n-j} - 1}{q^{k-j} - 1} \quad \text{and} \quad S(n) = \sum_{k=0}^n \binom{n}{k}_q. \quad (2)$$

It is natural to group codes in equivalence classes and thus ask the following question: when are two codes *essentially the same*? Informally speaking, we want two equivalent codes to be able to carry the same amount of information and to have the same error-correcting capabilities. There are three types of equivalence in coding theory: *permutation*, *monomial* and *semilinear* equivalence. The equivalence classes are the orbits of the action of three groups of transformations of $\mathbb{F}_q^n$, respectively, whose names correspond to the equivalence type they describe. We abuse terminology and call the equivalence classes also *inequivalent codes*.

The **permutation** group $\mathfrak{S}_n$ is formed by all the $n \times n$ permutation matrices, and the **monomial** group $\mathfrak{M}_n$ is the subgroup of $\text{GL}(\mathbb{F}_q^n)$ generated by $\mathfrak{S}_n$ and all diagonal matrices. These two groups inherit their action on $\mathbb{F}_q^n$ from $\text{GL}(\mathbb{F}_q^n)$, and since the image of a subspace via a linear transformation is a subspace of the same dimension, the action extends to $\mathcal{G}(n)$ and $\mathcal{G}(k, n)$. The **semilinear** group Γ_n is the semidirect product (also called *unrestricted wreath product*) of the group of field automorphisms $\text{Aut}(\mathbb{F}_q)$ of $\mathbb{F}_q$ and $\mathfrak{M}_n$:

$$\Gamma_n = \text{Aut}(\mathbb{F}_q) \ltimes \mathfrak{M}_n = \{(\sigma, M) \mid \sigma \in \text{Aut}(\mathbb{F}_q), M \in \mathfrak{M}_n\}.$$

The action of an element (M, σ) on a vector $x \in \mathbb{F}_q^n$ is the component-wise application of σ to x , followed by the usual action of M . This action too extends naturally to any Grassmannian and to the projective space. We will not spell out these group actions, for which we refer the reader to [12, Sections 1.6 and 1.7] and [1, Sections 1.4 and 1.5]. It is readily checked that, through suitable embeddings, $\mathfrak{S}_n \subseteq \mathfrak{M}_n \subseteq \Gamma_n$ and that if $q = p^h$ with p a prime, we have

$$|\mathfrak{S}_n| = n!, \quad |\mathfrak{M}_n| = n!(q-1)^n, \quad \text{and} \quad |\Gamma_n| = hn!(q-1)^n. \quad (3)$$

When $h = 1$, i.e. when $\mathbb{F}_q$ is a prime field, $\Gamma_n = \mathfrak{M}_n$; when $q = 2$, $\mathfrak{M}_n = \mathfrak{S}_n$, and the corresponding types of equivalence coincide. In particular, there is only one type of equivalence for binary linear codes. The notations $\mathfrak{S} = \mathfrak{S}_n$, $\mathfrak{M} = \mathfrak{M}_n$ and $\Gamma = \Gamma_n$ will be preferred when n is clear from context.

It can be checked that a semilinear transformation does not change the Hamming weight of a vector, and hence all the groups mentioned above are groups of *isometries* with respect to the Hamming metric. By the MacWilliams Extension Theorem [12, Section 7.9], every linear isometry of a code can be extended to a monomial transformation of the ambient space; this remains true for semilinear isometries and semilinear transformations [11]. It follows that the permutation/monomial/semilinear equivalence classes of linear codes are actually the *orbits* of the actions of the corresponding groups on $\mathcal{G}(n)$. Moreover, since the transformations are dimension-preserving, this also holds when considering the actions of the groups on $\mathcal{G}(k, n)$. For a group G acting on a set X , we denote by X/G the set of orbits of G in X . With this in mind, we define the following quantities that are the main subject of this paper's work.

Notation 2.1. Consider the action of $\mathfrak{M}_n$ described above. We introduce the quantities

$$\mathcal{N}_n^{\mathfrak{M}} = |\mathcal{G}(n)/\mathfrak{M}| \quad \text{and} \quad \mathcal{N}_{k(n),n}^{\mathfrak{M}} = |\mathcal{G}(k, n)/\mathfrak{M}|,$$

denoting respectively the number of monomial equivalence classes of codes, and the number of those classes having dimension $k = k(n)$. For $G = \mathfrak{S}_n$ (resp. Γ_n) we define the numbers $\mathcal{N}_n^{\mathfrak{S}}$ and $\mathcal{N}_{k(n),n}^{\mathfrak{S}}$ (resp. $\mathcal{N}_n^{\Gamma}$ and $\mathcal{N}_{k(n),n}^{\Gamma}$) analogously.

To avoid confusion, note that the numbers of equivalence classes in $\mathcal{G}(n)$ always have one index, while the numbers of inequivalent codes in $\mathcal{G}(k, n)$ always have two. This paper mainly focuses on the latter ones.

Problem statement. As mentioned in the introduction, the asymptotic behaviour of the numbers $\mathcal{N}_n^{\mathfrak{S}}$, $\mathcal{N}_n^{\mathfrak{M}}$ and $\mathcal{N}_n^{\Gamma}$ is known [9, 10, 11]. This paper studies the asymptotic behaviour of $\mathcal{N}_{k(n),n}^{\mathfrak{S}}$, $\mathcal{N}_{k(n),n}^{\mathfrak{M}}$ and $\mathcal{N}_{k(n),n}^{\Gamma}$ for fixed q and $n \rightarrow \infty$. We also consider the fraction that each of these numbers represents of the respective total number of equivalence classes. For example, in the monomial case we consider the quantity $\mathcal{N}_{k(n),n}^{\mathfrak{M}}/\mathcal{N}_n^{\mathfrak{M}}$. This problem is of its own interest for coding theorists, but it also links to combinatorics and probability theory.

3 Equivalence classes of codes with given dimension

In this section we show how the number of inequivalent linear codes of dimension $k = k(n)$ is asymptotically related to the q -binomial coefficient $\binom{n}{k(n)}_q$ as $n \rightarrow \infty$. We will understand this for the class of functions $k : \mathbb{N} \rightarrow \mathbb{N}$ that satisfy a particular property, which we denote by $(\star)$ and define in Proposition 3.1.

The general strategy that we follow to tackle the problem of counting inequivalent codes with a given dimension relies on a standard group-theoretic argument: we recall it quickly to establish notation, and for completeness. Let G be a group acting on a set X , where $g.x$ denotes the action of $g \in G$ on $x \in X$. For any $g \in G$, we denote by $\text{Fix}(g, X) = \{x \in X : g.x = x\}$ the set of g -invariant elements of X . The kernel of the action is the set $\Delta(G, X) = \{g \in G \mid \forall x \in X \ g.x = x\}$. By the Burnside Lemma then we have

$$|X/G| = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g, X)| = \frac{|\Delta(G, X)||X|}{|G|} + \sum_{g \in G \setminus \Delta(G, X)} |\text{Fix}(g, X)|, \quad (4)$$

and our results will rely on estimating the second sum on the RHS appropriately. We are especially interested in applying this result to the groups $\mathfrak{S}_n$, $\mathfrak{M}_n$, and Γ_n acting on $\mathcal{G}(k(n), n)$, similarly to what done in [9, 11] with their action on $\mathcal{G}(n)$.

We start by looking at monomial equivalence classes, and then consider permutation and semilinear classes as well.

3.1 Monomial equivalence classes

The starting point of our study is an application of the Burnside Lemma, which will be used repeatedly throughout the paper; see Equation (4) for the statement.

Proposition 3.1. *There exist positive constants A, ε such that, if $k : \mathbb{N} \rightarrow \mathbb{N}$ satisfies*

$$\lim_{n \rightarrow \infty} \frac{1}{4}n^2 - \varepsilon n + A\sqrt{n} - k(n)(n - k(n)) = -\infty, \quad (\star)$$

then

$$\mathcal{N}_{k(n), n}^{\mathfrak{M}} \sim \frac{\binom{n}{k(n)}_q}{n!(q-1)^{n-1}}, \quad \frac{\mathcal{N}_{k(n), n}^{\mathfrak{M}}}{\mathcal{N}_n^{\mathfrak{M}}} \sim p(k(n), n) := \frac{\binom{n}{k(n)}_q}{S(n)} \quad \text{as } n \rightarrow \infty.$$

Proof. For ease of notation, we write $k = k(n)$ and $\Delta = \Delta(\mathfrak{M}, \mathcal{G}(k, n)) = \{aI_n : a \in \mathbb{F}_q^*\}$, where I_n denotes the $n \times n$ identity matrix. Then $|\Delta| = q - 1$ and the Burnside Lemma implies

$$\begin{aligned} \mathcal{N}_{k, n}^{\mathfrak{M}} &= \frac{(q-1)|\mathcal{G}(k, n)| + \sum_{M \in \mathfrak{M} \setminus \Delta} |\text{Fix}(M, \mathcal{G}(k, n))|}{|\mathfrak{M}|} \\ &= \frac{(q-1)\binom{n}{k}_q + \sum_{M \in \mathfrak{M} \setminus \Delta} |\text{Fix}(M, \mathcal{G}(k, n))|}{n!(q-1)^n}. \end{aligned}$$

Since $\mathcal{G}(k, n) \subseteq \mathcal{G}(n)$ we have

$$\frac{\sum_{M \in \mathfrak{M} \setminus \Delta} |\text{Fix}(M, \mathcal{G}(k, n))|}{\binom{n}{k}_q} \leq \frac{\sum_{M \in \mathfrak{M} \setminus \Delta} |\text{Fix}(M, \mathcal{G}(n))|}{q^{k(n-k)}}.$$

From [9, Corollary 2.4 and Equation 4.1] we know that there exist positive constants A, ε such that, for n large enough,

$$\sum_{M \in \mathfrak{M} \setminus \Delta} |\text{Fix}(M, \mathcal{G}(n))| \in O\left(q^{\frac{1}{4}n^2 - \varepsilon n + A\sqrt{n}}\right). \quad (5)$$

If $\frac{1}{4}n^2 - \varepsilon n + A\sqrt{n} - k(n-k) \rightarrow -\infty$, by Equation (5) we have

$$\frac{\sum_{M \in \mathfrak{M} \setminus \Delta} |\text{Fix}(M, \mathcal{G}(n))|}{q^{k(n-k)}} \in o(1) \quad \text{as } n \rightarrow \infty.$$

It follows that

$$\mathcal{N}_{k,n}^{\mathfrak{M}} = \frac{\binom{n}{k}_q (q-1 + o(1))}{n!(q-1)^n} \sim \frac{\binom{n}{k}_q}{n!(q-1)^{n-1}} \quad \text{as } n \rightarrow \infty.$$

The second asymptotic estimate in the statement follows from [9, Theorem 4.1], since

$$\mathcal{N}_n^{\mathfrak{M}} \sim \frac{S(n)}{n!(q-1)^{n-1}} \quad \text{as } n \rightarrow \infty. \quad (6)$$

This concludes the proof. $\square$

Notation 3.1. Throughout the remainder of the paper, whenever condition $(\star)$ is mentioned, we implicitly mean that A and ε are the constants specified in the proof of the previous theorem.

Note that condition $(\star)$ excludes many classes of functions $k(n)$ that one could find interesting: for example, $k(n) = \alpha \in \mathbb{N}$ or $k(n) = \lambda n$, $0 < \lambda < 1/2$, do not satisfy $(\star)$. The following example outlines a class of functions $k(n)$ that *do* satisfy $(\star)$, and that will be of interest in the forthcoming analysis.

Example 3.1. Let r be a constant and $k(n) = \lfloor n/2 \rfloor - r$. Then $k(n)$ satisfies $(\star)$, since

$$k(n)(n - k(n)) = (\lfloor n/2 \rfloor - r)(\lceil n/2 \rceil + r) \geq \frac{1}{4}n^2 - \frac{1}{4} - r^2 - r.$$

A similar reasoning shows that $k(n) = \lceil n/2 \rceil + r$ satisfies $(\star)$ as well. These two functions will play a symmetric role in our analysis of the proportion of inequivalent codes having a given dimension (Section 5).

A more general class of functions $k(n)$ satisfying $(\star)$ is given in the following example.

Example 3.2. Generalising the previous example, a large class of functions $k(n)$ satisfying $(\star)$ can be found as follows. Write $k(n) = \lfloor n/2 \rfloor - \ell(n)$, with $\ell(n)$ a positive function. If $\ell(n) \in o((\varepsilon n - A\sqrt{n})^{1/2})$, then $k(n)$ satisfies $(\star)$, as we have

$$k(n)(n - k(n)) \geq \frac{1}{4}n^2 - \left(\ell(n) + \frac{1}{2} \right)^2.$$

For example, for $0 \leq \alpha < 1/2$, $\beta \in \mathbb{R}$, and $\ell(n) = n^\alpha \log n^\beta$, $k(n)$ satisfies $(\star)$.

The quantity $p(k, n)$, introduced in Proposition 3.1 plays a role also in the estimates for permutation and semilinear equivalence classes, as we see in the next subsection.

3.2 Permutation and semilinear classes

The analogue of Proposition 3.1 for permutation and semilinear equivalence classes of codes is the following result.

Proposition 3.2. *Let $q = p^h$, p a prime, and assume that $k : \mathbb{N} \rightarrow \mathbb{N}$ satisfies $(\star)$. Then for the permutation equivalence classes of codes we have*

$$\mathcal{N}_{k(n),n}^{\mathfrak{S}} \sim \frac{\binom{n}{k(n)}_q}{n!}, \quad \frac{\mathcal{N}_{k(n),n}^{\mathfrak{S}}}{\mathcal{N}_n^{\mathfrak{S}}} \sim p(k(n), n) \quad \text{as } n \rightarrow \infty.$$

For semilinear classes we have

$$\mathcal{N}_{k(n),n}^{\Gamma} \sim \frac{\binom{n}{k(n)}_q}{hn!(q-1)^{n-1}}, \quad \frac{\mathcal{N}_{k(n),n}^{\Gamma}}{\mathcal{N}_n^{\Gamma}} \sim p(k(n), n) \quad \text{as } n \rightarrow \infty.$$

Proof. As in the proof of Proposition 3.1, we let $k = k(n)$ and $\Delta = \Delta(\mathfrak{S}, \mathcal{G}(k, n))$ for ease of notation. Regarding permutation classes, by the Burnside Lemma we have (notice that in this case $\Delta = \{I_n\}$)

$$\mathcal{N}_{k,n}^{\mathfrak{S}} = \frac{|\mathcal{G}(k, n)| + \sum_{P \in \mathfrak{S} \setminus \Delta} |\text{Fix}(P, \mathcal{G}(k, n))|}{|\mathfrak{S}|} = \frac{\binom{n}{k}_q + \sum_{P \in \mathfrak{S} \setminus \Delta} |\text{Fix}(P, \mathcal{G}(k, n))|}{n!},$$

and since $\mathfrak{S} \subseteq \mathfrak{M}$ and k satisfies $(\star)$, we have

$$\frac{\sum_{P \in \mathfrak{S} \setminus \Delta} |\text{Fix}(P, \mathcal{G}(k, n))|}{\binom{n}{k}_q} \leq \frac{\sum_{M \in \mathfrak{M} \setminus \Delta} |\text{Fix}(M, \mathcal{G}(k, n))|}{\binom{n}{k}_q} \in o(1).$$

The rest of the proof is as in Proposition 3.1, replacing the asymptotic estimate for $\mathcal{N}_n^{\mathfrak{M}}$ of Equation (6) with the analogue result for $\mathcal{N}_n^{\mathfrak{S}}$ [9, Theorem 5.1], which tells us that

$$\mathcal{N}_n^{\mathfrak{S}} \sim \frac{S(n)}{n!} \quad \text{as } n \rightarrow \infty. \quad (7)$$

Concerning semilinear classes, we apply the Burnside Lemma in a slightly different fashion. By letting $\Delta = \Delta(\Gamma, \mathcal{G}(k, n))$, we have

$$\begin{aligned} \mathcal{N}_{k,n}^{\Gamma} &= \frac{1}{|\Gamma|} \sum_{M \in \mathfrak{M}} |\text{Fix}(M, \mathcal{G}(k, n))| + \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma \setminus \mathfrak{M}} |\text{Fix}(\gamma, \mathcal{G}(k, n))| \\ &= \frac{1}{h} \mathcal{N}_{k,n}^{\mathfrak{M}} + \frac{1}{|\Gamma|} \sum_{\gamma \in \Gamma \setminus \mathfrak{M}} |\text{Fix}(\gamma, \mathcal{G}(k, n))|. \end{aligned}$$

We estimate the second summand on the RHS using the results of [11, Section 2], from which it follows that there exists a positive constant ε' with the property that, for n large enough,

$$\sum_{\gamma \in \Gamma \setminus \mathfrak{M}} |\text{Fix}(\gamma, \mathcal{G}(n))| \in O\left(q^{\frac{1}{4}n^2 - \varepsilon'n^2}\right). \quad (8)$$

Therefore,

$$\frac{\sum_{\gamma \in \Gamma \setminus \mathfrak{M}} |\text{Fix}(\gamma, \mathcal{G}(k, n))|}{\binom{n}{k}_q} \leq \frac{\sum_{\gamma \in \Gamma \setminus \mathfrak{M}} |\text{Fix}(\gamma, \mathcal{G}(n))|}{q^{k(n-k)}} \in O\left(q^{\frac{1}{4}n^2 - \varepsilon' n^2 - k(n-k)}\right).$$

Notice that since k satisfies $(\star)$, we also have

$$\lim_{n \rightarrow \infty} \frac{1}{4}n^2 - \varepsilon' n^2 - k(n-k) = -\infty,$$

hence

$$\begin{aligned} \mathcal{N}_k^\Gamma \frac{hn!(q-1)^{n-1}}{\binom{n}{k}_q} &= \frac{1}{h} \mathcal{N}_k^\mathfrak{M} \frac{hn!(q-1)^{n-1}}{\binom{n}{k}_q} + \frac{hn!(q-1)^{n-1}}{|\Gamma|} \frac{\sum_{\gamma \in \Gamma \setminus \mathfrak{M}} |\text{Fix}(\gamma, \mathcal{G}(k, n))|}{\binom{n}{k}_q} \\ &\sim 1 + o(1) \sim 1. \end{aligned}$$

The statement about the fraction $\mathcal{N}_k^\Gamma / \mathcal{N}_n^\Gamma$ follows from [11, Equation 1.4], which tells us that

$$\mathcal{N}_n^\Gamma \sim \frac{1}{h} \mathcal{N}_n^\mathfrak{M} \sim \frac{S(n)}{hn!(q-1)^{n-1}} \quad \text{as } n \rightarrow \infty, \quad (9)$$

concluding the proof. $\square$

Remark 3.1. By comparing Proposition 3.1 and Proposition 3.2 one sees that the three quantities

$$\mathcal{N}_{k(n),n}^\mathfrak{S}, \quad \mathcal{N}_{k(n),n}^\mathfrak{M}, \quad \mathcal{N}_{k(n),n}^\Gamma$$

have different asymptotic behaviours, as expected from the definitions. Surprisingly instead, the fractions

$$\frac{\mathcal{N}_{k(n),n}^\mathfrak{S}}{\mathcal{N}_n^\mathfrak{S}}, \quad \frac{\mathcal{N}_{k(n),n}^\mathfrak{M}}{\mathcal{N}_n^\mathfrak{M}}, \quad \frac{\mathcal{N}_{k(n),n}^\Gamma}{\mathcal{N}_n^\Gamma}$$

are all asymptotically equivalent to $p(k(n), n)$ for n large. As we will see in Section 5, this enables a global asymptotic description of the proportion of inequivalent codes with a given dimension, regardless of the chosen notion of equivalence.

4 Asymptotics of the q -binomial and of $\mathcal{N}_{k(n),n}$

This section computes the asymptotic number of equivalence classes of codes of dimension $k = k(n)$, where $k(n)$ satisfies property $(\star)$ and $n \rightarrow \infty$; see Theorem 4.1 below. To achieve so, we start by studying the q -binomial coefficient n -choose- $k(n)$ and its asymptotic behaviour as n grows. Upper and lower bounds for the q -binomial coefficients are known: for every q and $0 \leq k \leq n$ we have

$$q^{k(n-k)} \leq \binom{n}{k}_q \leq \frac{1}{K_q} q^{k(n-k)}, \quad (10)$$

where $K_q = \prod_{j=1}^{\infty} (1 - q^{-j})$ is a finite constant depending only on q . The lower bound is easy to see, while for the upper bound we refer to [6]. Recall that K_q represents the fraction of

$n \times n$ matrices over $\mathbb{F}_q$ that are invertible as $n \rightarrow \infty$, and that $K_q = \phi(q^{-1})$, with ϕ the *Euler phi* function. The bounds in Equation (10) already tell us that $\binom{n}{k}_q \in O(q^{k(n-k)})$.

In the sequel, we are interested in determining a function $f_q : \mathbb{N} \rightarrow \mathbb{R}$ with the property that

$$\binom{n}{k(n)}_q \sim f_q(k(n))q^{k(n-k)} \quad \text{as } n \rightarrow \infty. \quad (11)$$

Note that by this we do *not* mean that the functions in Equation (11) converge. We begin by evaluating the ratio between two q -binomial coefficients. For every n and q , we refer to the q -binomial coefficient $\binom{n}{\lfloor n/2 \rfloor}_q = \binom{n}{\lceil n/2 \rceil}_q$ as the **central** q -binomial. The following two lemmata are cornerstones of this paper.

Lemma 4.1. *We have*

$$\frac{\binom{n}{k}_q}{\binom{n}{\lfloor n/2 \rfloor}_q} \sim \frac{K_q}{K_q(k)} q^{-(\lfloor n/2 \rfloor - k)(\lceil n/2 \rceil - k)} \quad \text{as } n \rightarrow \infty,$$

where $K_q(k) = \prod_{j=1}^k (1 - q^{-j})$ is the truncation of the product defining K_q to k terms. In particular,

$$\frac{K_q}{K_q(k)} \sim \begin{cases} 1 & \text{if } \lim_{n \rightarrow \infty} k(n) = +\infty, \\ \beta & \text{if } \lim_{n \rightarrow \infty} k(n) = \alpha < +\infty, \end{cases}$$

where α and β are constants and $\beta < 1$.

Proof. Let $\underline{m} = \lfloor n/2 \rfloor$, $\overline{m} = \lceil n/2 \rceil$; by symmetry of the q -binomial, we can assume $k \leq \underline{m}$ without loss of generality. Indeed, we always have $\min(k, n-k) \leq \underline{m}$ and $\binom{n}{k}_q = \binom{n}{n-k}_q$. Therefore,

$$\begin{aligned} \frac{\binom{n}{k}_q}{\binom{n}{\lfloor n/2 \rfloor}_q} &= \frac{\prod_{i=0}^{k-1} q^{n-i} - 1}{\prod_{j=0}^{k-1} q^{k-j} - 1} \frac{\prod_{j=0}^{\underline{m}-1} q^{\underline{m}-j} - 1}{\prod_{i=0}^{\underline{m}-1} q^{n-i} - 1} = \frac{\prod_{i=0}^{k-1} q^{n-i} - 1}{\prod_{j=1}^k q^j - 1} \frac{\prod_{j=1}^{\underline{m}} q^j - 1}{\prod_{i=0}^{\underline{m}-1} q^{n-i} - 1} \\ &= \frac{\prod_{j=k+1}^{\underline{m}} q^j - 1}{\prod_{i=k}^{\underline{m}-1} q^{n-i} - 1} = \frac{\prod_{j=1}^{\underline{m}-k} q^{k+j} - 1}{\prod_{i=\overline{m}+1}^{\underline{m}-k} q^i - 1} = \frac{\prod_{j=1}^{\underline{m}-k} q^{k+j} - 1}{\prod_{i=1}^{\underline{m}-k} q^{\overline{m}+i} - 1} \\ &= \prod_{j=1}^{\underline{m}-k} \frac{q^k}{q^{\overline{m}}} \frac{q^j - q^{-k}}{q^j - q^{-\overline{m}}} = q^{-(\overline{m}-k)(\underline{m}-k)} \prod_{j=1}^{\underline{m}-k} \frac{1 - q^{-(k+j)}}{1 - q^{-(\overline{m}+j)}}, \end{aligned}$$

and we are left with proving that

$$\prod_{j=1}^{\underline{m}-k} \frac{1 - q^{-(k+j)}}{1 - q^{-(\overline{m}+j)}} \sim \frac{K_q}{K_q(k)}.$$

We have that $\frac{K_q}{K_q(k)} = \prod_{j=1}^{\infty} (1 - q^{-(k+j)})$ and

$$\frac{\prod_{j=1}^{\infty} (1 - q^{-(k+j)})}{\prod_{j=1}^{\underline{m}-k} \frac{1 - q^{-(k+j)}}{1 - q^{-(\overline{m}+j)}}} = \prod_{j=1}^{\underline{m}-k} (1 - q^{-(\overline{m}+j)}) \prod_{j=1}^{\infty} (1 - q^{-(\underline{m}+j)}).$$

Note that

$$\begin{aligned} 1 &\geq \prod_{j=1}^{\underline{m}-k} (1 - q^{-(\overline{m}+j)}) \prod_{j=1}^{\infty} (1 - q^{-(\underline{m}+j)}) \geq \prod_{j=1}^{\infty} (1 - q^{-(\overline{m}+j)}) \prod_{j=1}^{\infty} (1 - q^{-(\underline{m}+j)}) \\ &\geq \left(\prod_{j=1}^{\infty} (1 - q^{-(\underline{m}+j)}) \right)^2. \end{aligned}$$

Taking the logarithm of the RHS we get

$$2 \log \left(\prod_{j=1}^{\infty} (1 - q^{-(\underline{m}+j)}) \right) = 2 \sum_{j=1}^{\infty} \log(1 - q^{-(\underline{m}+j)}).$$

For every fixed value of j we have $\lim_{n \rightarrow \infty} \log(1 - q^{-(\underline{m}+j)}) = 0$ and

$$|\log(1 - q^{-(\underline{m}+j)})| \leq \frac{q^{\underline{m}+j}}{q^{\underline{m}+j} - 1} - 1 = \frac{1}{q^{\underline{m}+j} - 1} \leq q^{-j}.$$

Since $\sum_{j=1}^{\infty} q^{-j} = (q - 1)^{-1} < \infty$, we can swap limit and sum to obtain

$$\lim_{n \rightarrow \infty} 2 \sum_{j=1}^{\infty} \log(1 - q^{-(\underline{m}+j)}) = 2 \sum_{j=1}^{\infty} \lim_{n \rightarrow \infty} \log(1 - q^{-(\underline{m}+j)}) = 0,$$

which implies $\lim_{n \rightarrow \infty} \prod_{j=1}^{\infty} (1 - q^{-(\underline{m}+j)}) = 1$ and

$$\prod_{j=1}^{\underline{m}-k} \frac{1 - q^{-(k+j)}}{1 - q^{1-(\overline{m}+j)}} \sim \frac{K_q}{K_q(k)},$$

which concludes our proof. $\square$

In the following result, we study the asymptotic growth of the central q -binomial. We separate this result from the previous lemma because we will use it independently also in the next section of the paper.

Lemma 4.2. *We have*

$$\frac{\binom{n}{\lfloor n/2 \rfloor}_q}{q^{\lfloor n/2 \rfloor \lceil n/2 \rceil}} \sim \frac{1}{K_q} \quad \text{as } n \rightarrow \infty.$$

Proof. Let $\underline{m} = \lfloor n/2 \rfloor$, $\overline{m} = \lceil n/2 \rceil$. Then

$$\begin{aligned} \frac{\binom{n}{\lfloor n/2 \rfloor}_q}{q^{\lfloor n/2 \rfloor \lceil n/2 \rceil}} &= \frac{\prod_{i=0}^{\underline{m}-1} \frac{q^{n-i}-1}{q^{\underline{m}-i}-1}}{q^{\underline{m}\overline{m}}} = \prod_{i=0}^{\underline{m}-1} \frac{q^{n-i}-1}{q^{\overline{m}}(q^{\underline{m}-i}-1)} \\ &= \prod_{i=0}^{\underline{m}-1} \frac{q^{\underline{m}-i} - q^{-\overline{m}}}{q^{\underline{m}-i} - 1} = \prod_{j=1}^{\underline{m}} \frac{q^j - q^{-\overline{m}}}{q^j - 1}, \end{aligned}$$

where $j = \underline{m} - i$. It follows that

$$\frac{\binom{n}{\underline{m}}_q}{K_q(\underline{m})q^{\underline{m}\overline{m}}} = \prod_{j=1}^{\underline{m}} (1 - q^{-(\overline{m}+j)}) \sim \prod_{j=1}^{\infty} (1 - q^{-(\overline{m}+j)}).$$

From the proof of Lemma 4.1 we know that

$$\prod_{j=1}^{\infty} (1 - q^{-(\overline{m}+j)}) \sim 1,$$

which gives the desired result. $\square$

Part of the previous result can be obtained using [8, Equation 6.2], which implies that

$$\binom{2m}{m}_q \sim \frac{q^{m^2}}{K_q}.$$

In other words, [8, Equation 6.2] can be used to show that the asymptotic result holds for the subsequence corresponding to even values of n , but not for the odd ones.

Combining the two lemmata we just proved, we obtain the following estimate for the asymptotic growth of the q -binomial coefficient.

Corollary 4.1. *We have*

$$\binom{n}{k(n)}_q \sim \frac{1}{K_q(k(n))} q^{k(n)(n-k(n))} \quad \text{as } n \rightarrow \infty.$$

Proof. Write $k = k(n)$ for ease of notation. By Lemmas 4.1 and 4.2 we have

$$\begin{aligned} \binom{n}{k}_q &= \frac{\binom{n}{k}_q}{\binom{n}{\lfloor n/2 \rfloor}_q} \frac{\binom{n}{\lfloor n/2 \rfloor}_q}{q^{\lfloor n/2 \rfloor \lceil n/2 \rceil}} q^{\lfloor n/2 \rfloor \lceil n/2 \rceil} \sim \frac{K_q}{K_q(k)K_q} q^{-(\lfloor n/2 \rfloor - k)(\lceil n/2 \rceil - k)} q^{\lfloor n/2 \rfloor \lceil n/2 \rceil} \\ &\sim \frac{1}{K_q(k)} q^{k(\lfloor n/2 \rfloor + \lceil n/2 \rceil) - k^2} = \frac{1}{K_q(k)} q^{k(n-k)}. \end{aligned} \quad \square$$

Remark 4.1. For $k = k(n)$ the above corollary can be made more specific if $\alpha = \lim_{n \rightarrow \infty} k(n)$ exists. If $\alpha < +\infty$, we have $K_q(k(n)) \rightarrow K_q(\alpha)$, while if $\alpha = +\infty$ we have $K_q(k(n)) \rightarrow K_q$. In other words, we have $f_q(k(n)) = 1/K_q(\alpha)$ or $f_q(k(n)) = 1/K_q$ in Equation (11).

The following theorem describes the asymptotic number of inequivalent codes of dimension $k = k(n)$ as $n \rightarrow \infty$. It is one of the main results of this work and represents a contribution of fundamental nature to coding theory.

Theorem 4.1. *Let $q = p^h$, p a prime, and assume $k(n)$ satisfies $(\star)$. Then for $n \rightarrow \infty$ we have*

$$\mathcal{N}_{k(n),n}^{\mathfrak{S}} \sim \frac{q^{k(n)(n-k(n))}}{K_q n!}, \quad \mathcal{N}_{k(n),n}^{\mathfrak{M}} \sim \frac{q^{k(n)(n-k(n))}}{K_q n! (q-1)^{n-1}}, \quad \mathcal{N}_{k(n),n}^{\Gamma} \sim \frac{q^{k(n)(n-k(n))}}{K_q h n! (q-1)^{n-1}}. \quad (12)$$

Proof. Apply Corollary 4.1 to the asymptotic results of Propositions 3.1 and 3.2 about the respective numbers of equivalence classes. Notice that, since $k(n)$ satisfies $(\star)$, we have $\lim_{n \rightarrow \infty} k(n) = +\infty$ and so $K_q(k(n)) \sim K_q$. $\square$

Example 4.1. By Example 3.1, we know that $k(n) = \lfloor n/2 \rfloor - r$ satisfies $(\star)$. Therefore the asymptotic number of monomially inequivalent codes of dimension $k(n)$ satisfies

$$\mathcal{N}_{k(n),n}^{\mathfrak{M}} \sim \frac{q^{\lfloor n/2 \rfloor \lceil n/2 \rceil - r^2}}{K_q n! (q-1)^{n-1}} \quad \text{as } n \rightarrow \infty.$$

By duality, this number should be equal to the one we obtain for $k(n) = \lceil n/2 \rceil + r$. It can be indeed checked that plugging this function into Equation (12) gives the same formulas.

5 Asymptotics of $S(n)$ and of $\mathcal{N}_{k(n),n}/\mathcal{N}_n$

We now turn to comparing the number of equivalence classes of codes with given dimension with the total number of equivalence classes of codes of *any* dimension, for sufficiently large length. As already shown in Propositions 3.1 and 3.2, this comparison boils down to investigating the asymptotic behaviour of the quantity $p(k, n) = \binom{n}{k}_q / S(n)$ for fixed q , $k = k(n)$ a function of the length and $n \rightarrow \infty$. We find out that, in general, one needs to consider two cases, given by the parity of n . In other words, it is not possible to describe the asymptotic behaviour of $p(k, n)$ with a single function. To overcome this technical issue, we look at the quantities $p^e(k, m) = p(k, 2m)$ and $p^o(k, m) = p(k, 2m+1)$ as $m \rightarrow \infty$, and we describe their asymptotic behaviour separately. When $k = k(n)$ satisfies $(\star)$, we can apply the analysis to compute the asymptotic proportion of equivalence classes of codes that have a given dimension, as desired.

For every value of m , the sum (over k) of the positive numbers $p(k, 2m)$ is 1, and the same holds for $p(k, 2m+1)$. This means they can be viewed as a probability distribution over $\mathbb{Z}$ (recall that $\binom{n}{k}_q = 0$ for $k \in \mathbb{Z} \setminus [0, n]$). Remarkably, and key for the results of this paper, when $k(n)$ is one of the functions in Example 3.1, our results show that these distributions have limit the Gaussian θ_3 and θ_2 distributions, respectively. Since the functions of Example 3.1 satisfy $(\star)$, this translates into an asymptotic description of the proportion of inequivalent codes that is particularly elegant. The following lemma completes Lemma 4.1 and Lemma 4.2 in forming the technical core of the paper. It describes the fundamental difference between n even and n odd when computing the asymptotic of $S(n)$, by looking at its ratio with the central binomial. This has two main consequences: first, it allows to describe the asymptotics of the two subsequences of $p(k, n)$ corresponding to even and odd values of n . Secondly, using this result we are able to describe the exact asymptotic behaviour of $S(n)$, a question left open in [18]. Upper and lower bounds for $S(n)$ are known. For instance, we have (see [7])

$$q^{\lfloor n/2 \rfloor \lceil n/2 \rceil} \leq S(n) < \frac{\theta_3(q^{-1}) + 1}{K_q} q^{\lfloor n/2 \rfloor \lceil n/2 \rceil}, \quad (13)$$

where $K_q = \prod_{j=1}^{\infty} (1 - q^{-j})$ already appeared in Equation (10) and $\theta_3(\cdot)$ is the *Jacobi* θ_3 constant, which we both now define. The **Jacobi** θ_2 and θ_3 constants are defined for $0 \leq w < 1$ as

$$\theta_2(w) = \sum_{k=-\infty}^{\infty} w^{(k+1/2)^2}, \quad \theta_3(w) = \sum_{k=-\infty}^{\infty} w^{k^2}. \quad (14)$$

In this paper, we are mainly interested in the values taken for $w = q^{-1}$. We can already see from Equation (13) that the θ_3 constant plays a role in bounding $S(n)$ from above; we will actually show that the θ_2 and θ_3 play a role in determining the exact asymptotic behaviour of $S(n)$.

Lemma 5.1. *We have*

$$\frac{\binom{n}{\lfloor n/2 \rfloor}_q}{S(n)} = \begin{cases} \frac{\binom{2m}{m}_q}{S_q(2m)} \sim \frac{1}{\theta_3(q^{-1})} & \text{if } n = 2m \text{ and } m \rightarrow \infty, \\ \frac{\binom{2m+1}{m}_q}{S_q(2m+1)} \sim \frac{1}{q^{1/4}\theta_2(q^{-1})} & \text{if } n = 2m+1 \text{ and } m \rightarrow \infty. \end{cases}$$

Proof. We first look at the case $n = 2m$. Define a sequence of functions

$$f_m(r) = \frac{\binom{2m}{m-r}_q}{\binom{2m}{m}_q}.$$

By Lemma 4.1 we have $\lim_{m \rightarrow \infty} f_m(r) = f(r) := q^{-r^2}$. Moreover for every r we have $0 \leq f_m(r) \leq q^{-|r|}$ and

$$\sum_{r=-\infty}^{+\infty} q^{-|r|} = \frac{3q-1}{q-1} < +\infty, \quad (15)$$

where we used $q \geq 2$. Thus by the Dominated Convergence Theorem,

$$\begin{aligned} \lim_{m \rightarrow \infty} \frac{S(2m, q)}{\binom{2m}{m}_q} &= \lim_{m \rightarrow \infty} \sum_{r=-m}^m \frac{\binom{2m}{m-r}_q}{\binom{2m}{m}_q} = \lim_{m \rightarrow \infty} \sum_{r=-\infty}^{\infty} \frac{\binom{2m}{m-r}_q}{\binom{2m}{m}_q} \\ &= \sum_{r=-\infty}^{\infty} \lim_{m \rightarrow \infty} \frac{\binom{2m}{m-r}_q}{\binom{2m}{m}_q} = \sum_{r=-\infty}^{\infty} \frac{1}{q^{r^2}} = \theta_3(q^{-1}), \end{aligned}$$

which is equivalent to our statement.

For $n = 2m+1$ the proof is similar: for every r we define a sequence of functions

$$f_m(r) = \frac{\binom{2m+1}{m-r}_q}{\binom{2m+1}{m}_q}.$$

Then by Lemma 4.1, $f_m(r)$ converges pointwise to $f(r) = q^{-r(r+1)}$ as $m \rightarrow \infty$. Moreover, for every r we have $0 \leq f_m(r) \leq q^{-|r|}$. Again by Equation (15) we have

$$\begin{aligned} \lim_{m \rightarrow \infty} \frac{S(2m+1, q)}{\binom{2m+1}{m}_q} &= \lim_{m \rightarrow \infty} \sum_{r=-m}^{m+1} \frac{\binom{2m+1}{m-r}_q}{\binom{2m+1}{m}_q} = \lim_{m \rightarrow \infty} \sum_{r=-\infty}^{+\infty} \frac{\binom{2m+1}{m-r}_q}{\binom{2m+1}{m}_q} \\ &= \sum_{r=-\infty}^{+\infty} \lim_{m \rightarrow \infty} \frac{\binom{2m+1}{m-r}_q}{\binom{2m+1}{m}_q} = \sum_{r=-\infty}^{\infty} \frac{1}{q^{r(r+1)}} = q^{1/4}\theta_2(q^{-1}). \end{aligned}$$

Taking reciprocals concludes our proof of the second part of the statement. $\square$

Lemma 5.1 allows us to isolate, and account for, the difference between n even and n odd when looking at the asymptotic behaviour of $p(k, n)$. This study is naturally completed using Lemma 4.1, as we now illustrate.

Theorem 5.1. *We have*

$$p^e(k, m) \sim \frac{K_q}{K_q(k)\theta_3(q^{-1})} q^{-(m-k)^2}, \quad p^o(k, m) \sim \frac{K_q}{K_q(k)\theta_2(q^{-1})} q^{-(m-k+1/2)^2} \quad \text{as } m \rightarrow \infty.$$

Proof. We have

$$p^e(k, m) = p(k, 2m) = \frac{\binom{2m}{m}_q \binom{2m}{k}_q}{S_q(2m) \binom{2m}{m}_q} \sim \frac{1}{\theta_3(q^{-1})} \frac{K_q}{K_q(k)} q^{-(m-k)^2}$$

by Lemma 4.1 and Lemma 5.1. The proof for $p^o(k, m)$ follows the same steps. $\square$

When $k = k(n)$ satisfies $(\star)$, our results allow for the description of the asymptotic proportion of inequivalent codes of dimension k , which is one of the centerpieces of this paper.

Corollary 5.1. *Assume that $k = k(n)$ satisfies $(\star)$. For $n = 2m$, $m \rightarrow \infty$, we have*

$$\frac{\mathcal{N}_{k(2m), 2m}^{\mathfrak{S}}}{\mathcal{N}_{2m}^{\mathfrak{S}}} \sim \frac{\mathcal{N}_{k(2m), 2m}^{\mathfrak{M}}}{\mathcal{N}_{2m}^{\mathfrak{M}}} \sim \frac{\mathcal{N}_{k(2m), 2m}^{\Gamma}}{\mathcal{N}_{2m}^{\Gamma}} \sim \frac{1}{\theta_3(q^{-1})} q^{-(m-k(2m))^2}.$$

For $n = 2m + 1$, $m \rightarrow \infty$, we have

$$\frac{\mathcal{N}_{k(2m+1), 2m+1}^{\mathfrak{S}}}{\mathcal{N}_{2m+1}^{\mathfrak{S}}} \sim \frac{\mathcal{N}_{k(2m+1), 2m+1}^{\mathfrak{M}}}{\mathcal{N}_{2m+1}^{\mathfrak{M}}} \sim \frac{\mathcal{N}_{k(2m+1), 2m+1}^{\Gamma}}{\mathcal{N}_{2m+1}^{\Gamma}} \sim \frac{1}{\theta_2(q^{-1})} q^{-(m-k(2m+1)+1/2)^2}.$$

Proof. Apply Theorem 5.1, noticing that if $k(n)$ satisfies $(\star)$, then $\lim_{n \rightarrow \infty} k(n) = +\infty$ and therefore $K_q/K_q(k(n)) \sim 1$. $\square$

Of particular interest in this paper is the case $k(n) = \lfloor n/2 \rfloor - r$ for some fixed $r \in \mathbb{N}$. For every n and q , we extend the definition of $p(k, n)$ to every $k \in \mathbb{Z}$ by setting $p(k, n) = 0$ whenever $k \notin [0, n]$. Since $0 \leq p(k, n) \leq 1$ for every $k \in \mathbb{Z}$ and $\sum_{k \in \mathbb{Z}} p(k, n) = 1$, the $p(k, n)$'s define a discrete probability distribution over $\mathbb{Z}$ via $\mathbb{P}(k) = p(k, n)$. We then consider the following shifts of the distributions:

1. if $n = 2m$, define a distribution on $\mathbb{Z}$ by $\mathbb{P}_m^e(r) = p_q^e(m - r, m)$;
2. if $n = 2m + 1$ is odd, define a distribution on $1/2 + \mathbb{Z}$ by $\mathbb{P}_m^o(r) = p_q^o(m - r + 1/2, m)$.

The two shifted distributions are symmetric with respect to 0, meaning $\mathbb{P}_m^e(r) = \mathbb{P}_m^e(-r)$ and $\mathbb{P}_m^o(r) = \mathbb{P}_m^o(-r)$ for every r and m . Informally, one can see r as a measure of the distance from the centre of the distribution. One of the main findings of this paper is that, as $m \rightarrow \infty$, the two distributions converge pointwise to the *discrete Gaussian* θ_3 and θ_2 distributions with nome $1/q$, studied in [17] in connection to the Brownian motion.

Definition 5.1. Let $w \in \mathbb{R}$, $0 < w < 1$, be a constant. The **discrete Gaussian θ_2 -distribution** is defined by the density

$$\mathbb{P}_{\theta_2}(k) = \frac{w^{k^2}}{\theta_2(w)}, \quad k \in \frac{1}{2} + \mathbb{Z},$$

whereas the **discrete Gaussian θ_3 -distribution** is defined by the density

$$\mathbb{P}_{\theta_3}(k) = \frac{w^{k^2}}{\theta_3(w)}, \quad k \in \mathbb{Z}.$$

The quantity w is called the **nome** of the distributions.

It was shown in [14] that the Gaussian θ_3 distribution is the *maximum entropy distribution* on $\mathbb{Z}$ having a specified mean and variance. This property qualifies the distribution as a discrete counterpart of the Gaussian distribution, which has the same characterisation over $\mathbb{R}$.

Remark 5.1. In [17], the θ_2 Gaussian is defined to take values in $\mathbb{Z}$ instead of $1/2 + \mathbb{Z}$. We shift the domain to have a distribution that is symmetric around 0. This also has the advantage of yielding a more concise formulation for the exponents of the nome.

We are interested in the case where the nome is $w = 1/q$. The following corollary spells out the convergence of the distributions $\mathbb{P}^e$ and $\mathbb{P}^o$. It is a straightforward consequence of our previous results, but nonetheless one of the most relevant findings of this work.

Corollary 5.2. *As $m \rightarrow \infty$ we have the following convergences in distribution:*

$$\mathbb{P}_m^e \rightarrow \mathbb{P}_{\theta_3} \quad \text{and} \quad \mathbb{P}_m^o \rightarrow \mathbb{P}_{\theta_2},$$

where the nome of the limit distributions is $1/q$.

Proof. For every fixed $r \in \mathbb{Z}$, by Theorem 5.1 and Corollary 5.1, we have

$$\mathbb{P}_m^e(r) = p_m^e(m - r, m) \sim \frac{q^{-r^2}}{\theta_3(1/q)} = \mathbb{P}_{\theta_3}(r),$$

and the result follows from the characterization of convergence in distribution in terms of pointwise convergence; see for instance [13]. The proof for $\mathbb{P}_m^o$ is analogous. $\square$

Stochastic characterisations for Gaussian θ_2 and θ_3 distributed random variables were proposed in [17]. These descriptions are based on infinite product representations of the θ_2 and θ_3 Jacobi theta functions, and involve the sum of infinitely many Bernoulli random variables with different distributions. A different characterisation for the Gaussian θ_3 distribution as the difference of Heine distributions was proposed in [14]. Corollary 5.2 offers an alternative result in this sense: as m grows, the distributions $\mathbb{P}_m^e(r)$ (resp. $\mathbb{P}_m^o(r)$) become increasingly good approximations of the Gaussian θ_3 (resp. θ_2), providing also an effective way to compute the values of the probabilities.

Answering an open question from [18]. Our results also allow for the description of the asymptotic behaviour of $S(n)$. It was shown in [18, Lemma 1] that for every q there exist constants $d_1 = d_1(q)$ and $d_2 = d_2(q)$ such that

$$S(2m+1) \sim d_1 q^{(2m+1)^2/4}, \quad S(2m) \sim d_2 q^{(2m)^2/4} \quad \text{as } m \rightarrow \infty.$$

In the same work, it is shown that $d_1 < 1 \leq d_2$ for $q \geq 49$, and that $d_1 < d_2$ for all $q < 49$, implying that the two values never coincide. Yet, the two numbers are not computed explicitly. From Equation (13) it is evident that $d_2 \leq \frac{\theta_3(1/q)+1}{K_q}$. Furthermore, our results imply closed formulas for the constants d_1 and d_2 as in the following result.

Corollary 5.3. *We have*

$$S(2m) \sim \frac{\theta_3(1/q)}{K_q} q^{m^2} \quad \text{and} \quad S(2m+1) \sim \frac{\theta_2(1/q)}{K_q} q^{(m+1/2)^2}$$

Proof. Simply combine Lemma 5.1 and Lemma 4.2. □

Therefore, in the notation of [18], we have $d_1 = \frac{\theta_2(1/q)}{K_q}$ and $d_2 = \frac{\theta_3(1/q)}{K_q}$.

References

- [1] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann. *Error-correcting linear codes: Classification by isometry and applications*. Springer, 2006.
- [2] J. E. Bonin. Automorphism groups of higher-weight Dowling geometries. *Journal of Combinatorial Theory, Series B*, 58(2):161–173, 1993.
- [3] J. E. Bonin. Modular elements of higher-weight Dowling lattices. *Discrete mathematics*, 119(1-3):3–11, 1993.
- [4] N. G. De Bruijn. *Asymptotic methods in analysis*. Courier Corporation, 2014.
- [5] T. A. Dowling. Codes, Packings and the Critical Problem. Technical report, 1971.
- [6] M. Gadouleau and Z. Yan. On the decoder error probability of bounded rank-distance decoders for maximum rank distance codes. *IEEE Transactions on Information Theory*, 54(7):3202–3206, 2008.
- [7] M. Gadouleau and Z. Yan. Packing and covering properties of subspace codes for error control in random linear network coding. *IEEE Transactions on Information Theory*, 56(5):2097–2108, 2010.
- [8] A. Gruica and A. Ravagnani. Common complements of linear subspaces and the sparseness of MRD codes. *SIAM Journal on Applied Algebra and Geometry*, 6(2):79–110, 2022.
- [9] X.-D. Hou. On the asymptotic number of non-equivalent q -ary linear codes. *Journal of Combinatorial Theory, Series A*, 112(2):337–346, 2005.
- [10] X.-D. Hou. On the asymptotic number of non-equivalent binary linear codes. *Finite Fields and Their Applications*, 13(2):318–326, 2007.

- [11] X.-D. Hou. Asymptotic numbers of non-equivalent codes in three notions of equivalence. *Linear and Multilinear Algebra*, 57(2):111–122, 2009.
- [12] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge university press, 2010.
- [13] J. Jacod and P. Protter. *Probability essentials*. Springer Science & Business Media, 2004.
- [14] A. W. Kemp. Characterizations of a discrete normal distribution. *Journal of Statistical Planning and Inference*, 63(2):223–229, 1997.
- [15] R. F. Lax. On the character of S_n acting on subspaces of $\mathbb{F}_q^n$. *Finite Fields and Their Applications*, 10(3):315–322, 2004.
- [16] A. Ravagnani. Whitney numbers of combinatorial geometries and higher-weight Dowling lattices. *SIAM Journal on Applied Algebra and Geometry*, 6(2):156–189, 2022.
- [17] P. Salminen and C. Vignat. Probabilistic aspects of Jacobi theta functions. *Mathematica Scandinavica*, 130(3), 2024.
- [18] M. Wild. The asymptotic number of inequivalent binary codes and nonisomorphic binary matroids. *Finite Fields and their Applications*, 6(2):192–202, 2000.