Decoding of Lifted Affine-Invariant Codes

Lukas Holzbaur* and Nikita Polyanskii*†
*Technical University of Munich, Germany
†Skolkovo Institute of Science and Technology, Russia
Emails: lukas.holzbaur@tum.de, nikita.polyansky@gmail.com

Abstract—**Lifted Reed-Solomon codes, a subclass of lifted affine-invariant codes, have been shown to be of high rate while preserving locality properties similar to generalized Reed-Muller codes, which they contain as subcodes. This work introduces a simple bounded distance decoder for (subcodes of) lifted affine-invariant codes that is guaranteed to decode up to half of an asymptotically tight bound on their minimum distance. Further, long q-ary lifted affine-invariant codes are shown to correct almost all error patterns of relative weight $\frac{q-1}{q} - \varepsilon$ for $\varepsilon > 0$.**

I. INTRODUCTION

Binary and q-ary Reed-Muller (RM) codes are among the oldest and best studied classes of codes. Their long-standing popularity is partially due to their good locality properties, guaranteeing linear dependencies between many small subsets of codeword symbols. Lifted Reed-Solomon (RS) and, more generally, lifted affine-invariant codes preserve this attribute, but simultaneously allow for an increased code rate compared to RM codes. Informally, the lift of an affine-invariant code (base code) is defined to be the set of all functions for which the restriction to any affine subspace of a fixed dimension is in the base code. Exploiting this structure has led to results that are of interest in a wide array of applications, including error-correction algorithms via majority logic decoding [1, Ch. 13], locally decodable and testable codes [2], batch codes [3], low-degree testing [4], and list decoding [5], [6].

While these properties naturally lead to local decoding algorithms, i.e., randomized approaches to correctly recover a single symbol with high probability, they can also be exploited to design algorithms for the recovery of the entire codeword symbol-by-symbol through aggregation of the local decoding results. In Section III, we present such a deterministic bounded distance (BD) decoding algorithm for lifted affine-invariant codes. As long as the base code admits an efficient unique decoding algorithm, this decoder runs in polynomial time and is guaranteed to recover the codeword correctly for errors of weight up to half of an asymptotically tight bound on their minimum distance. Then, in Section IV, we analyse a fast randomized decoder for long q-ary codes constructed by lifting a fixed affine-invariant code. A random pattern of errors with relative weight less than $\frac{q-1}{q} - \varepsilon$ is shown to be correctable with probability at least $1 - \delta$, where δ can be exponentially small in length, in time $\log \frac{1}{\delta} \operatorname{poly}(\varepsilon^{-1})$. This resembles behaviour of randomized decoders for low-rate binary RM codes shown in [7], [8].

The presented results can be applied to both generalized (q-ary) RM codes and lifted RS. A q-ary RM code $\mathcal{RM}_q(u, m)$ consists of all m-variate polynomials of degree at most u with coefficients in $\mathbb{F}_q$. Non-binary RM codes were introduced by separate groups of authors in [9], [10], [11] and shown to be subfield subcodes of RS codes over $\mathbb{F}_{q^m}$ [10]. Thus, any decoding algorithm for RS codes can be used to decode RM codes. Randomized list-decoding algorithms for RM codes were proposed in [5], [4], [6] and three deterministic list-decoders for Reed-Muller codes running in polynomial time were introduced in [12]. Two of the latter view RM codes as subfield subcodes of RS codes and can decode beyond half the minimum distance requiring a polynomial number of field operations in the large field $\mathbb{F}_{q^m}$. An approach for a global decoding algorithm of RM codes based on local decoding has been discussed in [13].

Let $\mathcal{F} = \mathcal{RM}_q(u, 1)$ and note that the code $\mathcal{F}$ is an RS code. Clearly, for $u < q$ the code $\mathcal{RM}_q(u, m)$ is a subcode of the lifted RS code $\mathcal{L}(\mathcal{F})$, as introduced in [2]. It is known [2], [3] that for fixed m and large q, the rate of lifted RS codes approaches one, whereas the rate of non-binary RM codes does not exceed $1/m!$. Surprisingly, similar to RM codes, they can also be seen [14] as subfield subcodes of (low-degree) RS codes and thereby (list-)decoded by RS (list-)decoders over $\mathbb{F}_{q^m}$. Applying the decoder introduced in this work to lifted RS codes requires $n^2 \operatorname{poly}(\log q)$ operations in $\mathbb{F}_q$ (see Theorem 1), given a BMD decoder for the (q-ary) RS base code running in $q \operatorname{poly}(\log q)$ (see, e.g., [15]) and guarantees to decode up to half of an asymptotically tight bound on their minimum distance, as bounded in [2, Lemma 5.7] (see Lemma 1).

II. PRELIMINARIES

We start by introducing some notation that is used throughout the paper. Let $[n]$ be the set of integers from 1 to n. A vector is denoted by bold lowercase letters such as $\mathbf{d}$. Let $q := p^l$ for a prime integer p and a positive integer l. Let $\mathbb{F}_q$ be a field of order q and $\mathbb{F}_q^*$ denote the multiplicative group of the field. By $\mathbb{Z}_q$ denote the ring of integers modulo q.

For an arbitrary set D, a set of functions $\mathcal{F} \subseteq \{D \to \mathbb{F}_q\}$ is said to be a *code* defined over the domain D. The code is called a *linear* $[n, k]_q$-code with $n := |D|$ and $k = \dim_{\mathbb{F}_q}(\mathcal{F}) := \log_q |\mathcal{F}|$ if for any $f, g \in \mathcal{F}$ and $\lambda \in \mathbb{F}_q$, the function $\lambda f + g$ belongs to $\mathcal{F}$. In this paper, we will mainly consider the domain $D = \mathbb{F}_Q^t$, where $\mathbb{F}_Q$ is an extension field of $\mathbb{F}_q$. In this case, for any $f \in \mathcal{F}$, there exists a unique polynomial (of degree at most $Q - 1$ in each variable) in the ring of

polynomials in t variables with coefficients in $\mathbb{F}_Q$, denoted as $\mathbb{F}_Q[x_1, \ldots, x_t]$ or $\mathbb{F}_Q[\mathbf{x}]$, corresponding to the function f. Thus, f can be represented as $\sum_{\mathbf{d} \in \mathbb{Z}_Q^t} f_{\mathbf{d}} \mathbf{x}^{\mathbf{d}}$, where $\mathbf{x}^{\mathbf{d}} = \prod_{i=1}^m x_i^{d_i}$ and $f_{\mathbf{d}} \in \mathbb{F}_Q$. By $\mathrm{Deg}(f)$ denote the set of tuples $\mathbf{d}$ such that $f_{\mathbf{d}} \neq 0$. We also define the *degree set* of the code $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$, written as $\mathrm{Deg}(\mathcal{F})$, to be the union of $\mathrm{Deg}(f)$ with $f \in \mathcal{F}$. For any $f : D \to \mathbb{F}_q$, define its *weight* to be $\mathrm{wt}(f) := |\{a \in D : f(a) \neq 0\}|$. The *distance* between two functions $f, g : D \to \mathbb{F}_q$ is defined as $d(f, g) := \mathrm{wt}(f - g)$. The *minimal distance* in the code $\mathcal{F}$ is then $d_{\mathcal{F}} := \min\{d(f, g) : f, g \in \mathcal{F}, f \neq g\}$. For a function $f : \mathbb{F}_Q^m \to \mathbb{F}_q$ and a set $S \subseteq \mathbb{F}_Q^m$, denote by $f|_S$ the *restriction* of f to the domain S, i.e., $f|_S : S \to \mathbb{F}_q$.

Consider a code $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$. Suppose that there exists a decoder $\mathfrak{D}$ that takes an arbitrary function $g : \mathbb{F}_Q^t \to \mathbb{F}_q \cup \{*\}$ as an input and outputs either a function from $\mathcal{F}$, or an error message. We say that $\mathfrak{D}$ *recovers* $\mathcal{F}$ from e errors and r erasures, if for any $g : \mathbb{F}_Q^t \to \mathbb{F}_q \cup \{*\}$ with $S = g^{-1}(*)$, $|S| \leq r$, and $f \in \mathcal{F}$ with $d(f|_{\mathbb{F}_Q^t \setminus S}, g|_{\mathbb{F}_Q^t \setminus S}) \leq e$, the result of decoding is correct, i.e., $\mathfrak{D}(g) = f$.

Consider a code $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$. A function $A : \mathbb{F}_Q^t \to \mathbb{F}_Q^t$ is called *affine* if $A(\mathbf{x})$ can be represented as $M\mathbf{x} + \mathbf{b}$ for some matrix $M \in \mathbb{F}_Q^{t \times t}$ and vector $\mathbf{b} \in \mathbb{F}_Q^t$. If M is nondegenerate, then A is said to be an *affine permutation*. The code $\mathcal{F}$ is said to be *affine-invariant* if for every affine permutation function $A : \mathbb{F}_Q^t \to \mathbb{F}_Q^t$ and for every $f(\mathbf{x}) \in \mathcal{F}$, the function $f(A(\mathbf{x}))$ belongs to $\mathcal{F}$. Many important properties of affine-invariant codes were derived in [16], [17], [2].

For a fixed basis $\{\boldsymbol{\gamma}_1, \ldots, \boldsymbol{\gamma}_t\}$ of a t-dimensional vector space V over $\mathbb{F}_Q^m$ define the linear map $\varphi_V : V \mapsto \mathbb{F}_Q^t$ by

$$\varphi_V \left(\sum_{j=1}^t \lambda_j \boldsymbol{\gamma}_j \right) = (\lambda_1, \ldots, \lambda_t) \in \mathbb{F}_Q^t.$$

For a function $g : \mathbb{F}_Q^m \to \mathbb{F}_q$ and an affine subspace $V + \mathbf{a}$, where $\mathbf{a} \in \mathbb{F}_Q^m$, define the function $g_{\mathbf{a}}^{(V)} : \mathbb{F}_Q^t \to \mathbb{F}_q$ as

$$g_{\mathbf{a}}^{(V)}(\mathbf{y}) := g(\varphi_V^{-1}(\mathbf{y}) + \mathbf{a}). \tag{1}$$

Note that, $g_{\mathbf{a}'}^{(V)}(\mathbf{y}) = g_{\mathbf{a}}^{(V)}(\mathbf{y} + \varphi_V(\mathbf{a}' - \mathbf{a})) \; \forall \; \mathbf{a}, \mathbf{a}' \in V$.

Definition 1 (Lifted Affine-Invariant Code, [2, Definition 1.1]). *Let $\mathcal{F}$ be an affine-invariant code $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$. The lifted code $\mathcal{L}(\mathcal{F}) \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$ is the set of functions f such that $f_{\mathbf{a}}^{(V)} \in \mathcal{F}$ for any t-dimensional affine subspace $V + \mathbf{a} \subset \mathbb{F}_Q^m$.*

Lemma 1 ([2, Lemma 5.7]). *Let $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ be an affine-invariant code of relative distance $d_{\mathcal{F}}$. Then the distance $d_{\mathcal{L}(\mathcal{F})}$ of the lifted code $\mathcal{L}(\mathcal{F}) \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$ as in Definition 1 is bounded by*

$$(d_{\mathcal{F}} - 1) \frac{Q^m}{Q^t - 1} < d_{\mathcal{L}(\mathcal{F})} \leq d_{\mathcal{F}} Q^{m-t}.$$

III. BOUNDED DISTANCE DECODING

In this section we introduce a simple bounded distance decoder for lifted affine-invariant codes. The main principle is based on the fact that, by definition, the restriction of a lifted affine-invariant code $\mathcal{L}(\mathcal{F})$ to any affine subspace belongs to

the code $\mathcal{F}$. Assuming a fixed value at one position, we derive the minimal number of positions in which two functions would have to disagree for the decoding of these restrictions to give the respective result. We then show that, if the number of such positions is within the decoding radius, the value that results in the lowest number, must be the correct value of the function at this position.

Fix a (partial) spread of $\mathbb{F}_Q^m$, treated as an m-dimensional vector space, into t-dimensional subspaces $V_1, \ldots, V_s \subset \mathbb{F}_Q^m$ (e.g., see [18]), i.e., $V_i \cap V_j = \mathbf{0}$ for $i \neq j$ and

$$s = \begin{cases} \frac{Q^m - 1}{Q^t - 1}, & \text{if } t \mid m, \\ Q^{m-t}, & \text{if } t \nmid m. \end{cases} \tag{2}$$

Definition 2. *For $1 \leq t < m/2$, let $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ be an affine-invariant code of distance $d_{\mathcal{F}}$. Define $e := \lfloor \frac{d_{\mathcal{F}} - 1}{2} \rfloor$. Consider a function $g : \mathbb{F}_Q^m \to \mathbb{F}_q$ and let $g_{\mathbf{a}}^{(V_i)}$ be as in (1). For any point $\mathbf{a} \in \mathbb{F}_Q^m$, field element $\alpha \in \mathbb{F}_q$, and integer $j \in \{0, 1, \ldots, e\}$, define $M_{\mathbf{a}}(\alpha, j)$ to be the number of affine subspaces of the form $\mathbf{a} + V_i$ such that there exists [1] a $\hat{g}_{\mathbf{a}}^{(V_i)} \in \mathcal{F}$ with $\hat{g}_{\mathbf{a}}^{(V_i)}(\mathbf{0}) = \alpha$ and*

- $d(g_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \setminus \mathbf{0}}, \hat{g}_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \setminus \mathbf{0}}) = j$, *if $d_{\mathcal{F}}$ is even,*
- $d(g_{\mathbf{a}}^{(V_i)}, \hat{g}_{\mathbf{a}}^{(V_i)}) = j$, *if $d_{\mathcal{F}}$ is odd.* $\quad (3)$

Further, define $M_{\mathbf{a}}(\star)$ to be the number of affine subspaces $\mathbf{a} + V_i$ for which no $\hat{g}_{\mathbf{a}}^{(V_i)} \in \mathcal{F}$ that satisfies (3) exists for any $\alpha \in \mathbb{F}_q$ and $j \in \{0, 1, \ldots, e\}$. For $\alpha \in \mathbb{F}_q$, denote

$$\delta_{\mathbf{a}}(\alpha) := \begin{cases} \mathbb{1}\{g(\mathbf{a}) \neq \alpha\}, & \text{if } d_{\mathcal{F}} \text{ is odd} \\ 0, & \text{if } d_{\mathcal{F}} \text{ is even.} \end{cases}$$

For $\mathbf{a} \in \mathbb{F}_Q^m$ and $\alpha \in \mathbb{F}_q$, define

$$N_{\mathbf{a}}(\alpha) := \mathbb{1}\{g(\mathbf{a}) \neq \alpha\} + \sum_{j=0}^e (j - \delta_{\mathbf{a}}(\alpha)) M_{\mathbf{a}}(\alpha, j)$$

$$+ \sum_{\beta \neq \alpha} \sum_{j=0}^e (d_{\mathcal{F}} - 1 - j + \delta_{\mathbf{a}}(\beta)) M_{\mathbf{a}}(\beta, j)$$

$$+ (e + 1 - \delta_{\mathbf{a}}(\alpha)) M_{\mathbf{a}}(\star).$$

With Definition 2 we can express the distance between two functions in terms of the distances between their respective restrictions to affine subspaces, given by $N_{\mathbf{a}}(\alpha)$.

Lemma 2. *Let $\mathcal{F}$, g, and $N_{\mathbf{a}}(\alpha)$ be as in Definition 2 and $\mathcal{L}(\mathcal{F}) \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$ be a lifted code as in Definition 1. Then for any $\mathbf{a} \in \mathbb{F}_Q^m$, $\alpha \in \mathbb{F}_q$, and $f \in \mathcal{L}(\mathcal{F})$ with $f(\mathbf{a}) = \alpha$ it holds that $d(f, g) \geq N_{\mathbf{a}}(\alpha)$.*

Proof. Given the point $\mathbf{a} \in \mathbb{F}_Q^m$, we count the number of positions that must differ between f and g given the values of $M_{\mathbf{a}}(\beta, j)$, $\forall \beta \in \mathbb{F}_q$, $\forall j \in \{0, 1, \ldots, e\}$, and $M_{\mathbf{a}}(\star)$. Recall that $M_{\mathbf{a}}(\beta, j)$ is the number of affine subspaces $\mathbf{a} + V_i$ for which $\hat{g}_{\mathbf{a}}^{(V_i)}(\mathbf{0}) = \beta$ and (3) holds. By definition, these affine subspaces intersect *only* in $\mathbf{a}$ and the sum over all $M_{\mathbf{a}}(\beta, j)$

---

[1] Note that by definition of e there exists at most one such function in $\mathcal{F}$.

is the number of affine subspaces of the form $\mathbf{a} + V_i$, i.e.,

$$\sum_{\beta,j} M_{\mathbf{a}}(\beta, j) + M_{\mathbf{a}}(\star) = s, \qquad (4)$$

for s as in (2). Hence, the distance between f and g is lower bounded by

$$d(f,g) \geq \mathbb{1}\{f(\mathbf{a}) \neq g(\mathbf{a})\} + \sum_{i=1}^{s} d(f_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \mathbf{0}}, g_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \mathbf{0}}).$$

As $f(\mathbf{a}) = \alpha$ by assumption, we have $\mathbb{1}\{f(\mathbf{a}) \neq g(\mathbf{a})\} = \mathbb{1}\{g(\mathbf{a}) \neq \alpha\}$. For the remaining positions, first consider the case of odd $d_{\mathcal{F}}$. For all affine subspaces contributing to $M(\alpha, j)$, where $j \leq e$, we have

$$d(f_{\mathbf{a}}^{(V_i)}, g_{\mathbf{a}}^{(V_i)}) \geq \begin{cases} j, & \text{if } \hat{g}_{\mathbf{a}}^{(V_i)} = f_{\mathbf{a}}^{(V_i)}, \\ d_{\mathcal{F}} - t \geq j, & \text{else.} \end{cases} \qquad (5)$$

Excluding point $\mathbf{a}$ in f and g, i.e., the origin in the restrictions to $\mathbf{a} + V_i$, we obtain

$$d(f_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}, g_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}) \geq j - \mathbb{1}\{g_{\mathbf{a}}^{(V_i)}(\mathbf{0}) \neq \alpha\} .$$

Now consider the affine subspaces contributing to $M(\beta, j)$ with $\beta \neq \alpha$. As $f_{\mathbf{a}}^{(V_i)}, \hat{g}_{\mathbf{a}}^{(V_i)} \in \mathcal{F}$ and $f_{\mathbf{a}}^{(V_i)}(\mathbf{0}) = \alpha \neq \beta = \hat{g}_{\mathbf{a}}^{(V_i)}(\mathbf{0})$, we have $d(f_{\mathbf{a}}^{(V_i)}, \hat{g}_{\mathbf{a}}^{(V_i)}) \geq d_{\mathcal{F}}$. Therefore

$$d(f_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}, \hat{g}_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}) \geq d_{\mathcal{F}} - \underbrace{\mathbb{1}\{f_{\mathbf{a}}^{(V_i)}(\mathbf{0}) \neq g_{\mathbf{a}}^{(V_i)}(\mathbf{0})\}}_{=1}.$$

Further, we have $d(g_{\mathbf{a}}^{(V_i)}, \hat{g}_{\mathbf{a}}^{(V_i)}) = j$ and

$$d(g_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}, \hat{g}_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}) = j - \mathbb{1}\{g_{\mathbf{a}}^{(V_i)}(\mathbf{0}) \neq \beta\}.$$

By the triangle inequality we get

$$d(f_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}, g_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}) \geq d_{\mathcal{F}} - 1 - j + \mathbb{1}\{g_{\mathbf{a}}^{(V_i)}(\mathbf{0}) \neq \beta\}.$$

Finally, as $f_{\mathbf{a}}^{(V_i)} \in \mathcal{F}$, a necessary condition for an affine subspace to contribute to $M_{\mathbf{a}}(\star)$ is $d(g_{\mathbf{a}}^{(V_i)}, f_{\mathbf{a}}^{(V_i)}) \geq e + 1$. Again, excluding position $\mathbf{a}$ we get

$$d(g_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}, f_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}) \geq e + 1 - \underbrace{\mathbb{1}\{f_{\mathbf{a}}^{(V_i)}(\mathbf{0}) \neq g_{\mathbf{a}}^{(V_i)}(\mathbf{0})\}}_{=\mathbb{1}\{g_{\mathbf{a}}^{(V_i)}(\mathbf{0}) \neq \alpha\}} .$$

By the same arguments, we obtain the lower bounds for even $d_{\mathcal{F}}$. The only difference to the case of odd $d_{\mathcal{F}}$ is that the erasure placed in position $\hat{g}_{\mathbf{a}}^{(V_i)}(\mathbf{0})$ means that none of the j errors can be in position $\mathbf{a}$.

The lemma statement follows from observing that $N_{\mathbf{a}}(\alpha)$ is defined as the weighted sum over these cases. $\qquad \square$

Definition 3. *For $1 \leq t < m/2$, let $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ be an affine-invariant code of distance $d_{\mathcal{F}}$. Let $\mathcal{L}(\mathcal{F}) \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$ be a lifted code as in Definition 1. We define*

$$d_{\text{low}} := \begin{cases} (d_{\mathcal{F}} - 1)\frac{Q^m - 1}{Q^t - 1} + 1, & \text{if } t \mid m. \\ (d_{\mathcal{F}} - 1)Q^{m-t} + 1, & \text{otherwise.} \end{cases}$$

Remark 1. *Note that by [2, Lemma 5.7] (see Lemma 1) we have $d_{\mathcal{L}(\mathcal{F})} \geq d_{\text{low}}$. Further, as $t \mid m$ implies $Q^t - 1 \mid Q^m - 1$, it is easy to check that d_{low} coincides with the lower bound of [2, Lemma 5.7] in this case. On the other hand, d_{low} is slightly lower if $t \nmid m$, due to the fact that [2, Lemma 5.7] employs*

arguments based on all *affine subspaces passing through a point, while d_{low} can be obtained by only considering a partitioning of $\mathbb{F}_Q^m$ into a (partial) spread, as will be shown in the proof of Theorem 1.*

It remains to show the existence of a BD decoder based on the distance measure introduced in Lemma 2.

Theorem 1. *For $1 \leq t < m/2$, let $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$ be an affine-invariant code of distance $d_{\mathcal{F}}$ and $\mathfrak{D}'$ be a decoder recovering $\mathcal{F}$ from $e := \lfloor \frac{d_{\mathcal{F}} - 1}{2} \rfloor$ errors and, if $d_{\mathcal{F}}$ is even, from one erasure. Let $\mathcal{L}(\mathcal{F}) \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$ be a lifted code as in Definition 1 and let d_{low} be as in Definition 3.*

Then, there exists a decoder $\mathfrak{D}$ that recovers $\mathcal{L}(\mathcal{F})$ from $e_{\text{low}} := \lfloor \frac{d_{\text{low}} - 1}{2} \rfloor$ errors in time $O(Q^{2m-t}T(\mathfrak{D}'))$ and $O(Q^{2m-2t}T(\mathfrak{D}'))$ for even and odd distance $d_{\mathcal{F}}$, respectively.

Proof. For completeness, we include a short proof that $d_{\mathcal{L}(\mathcal{F})} \geq d_{\text{low}}$, as it is closely related to the principle of the presented decoder. Let $f, \tilde{f} \in \mathcal{L}(\mathcal{F})$ and assume $f(\mathbf{a}) \neq \tilde{f}(\mathbf{a})$. As the affine subspaces $\mathbf{a} + V_1, ..., \mathbf{a} + V_s$ intersect only in $\mathbf{a}$, we have

$$d(f,g) \geq \mathbb{1}\{f(\mathbf{a}) \neq \tilde{f}(\mathbf{a})\} + \sum_{i=1}^{s} d(f_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}, \tilde{f}_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}).$$

By Definition 1 we have $f_{\mathbf{a}}^{(V_i)}, \tilde{f}_{\mathbf{a}}^{(V_i)} \in \mathcal{F}$. Further, as $f(\mathbf{a}) \neq \tilde{f}(\mathbf{a})$, we have $f_{\mathbf{a}}^{(V_i)} \neq \tilde{f}_{\mathbf{a}}^{(V_i)}$, so

$$d(f_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}, \tilde{f}_{\mathbf{a}}^{(V_i)}|_{\mathbb{F}_Q^t \backslash \{\mathbf{0}\}}) \geq d_{\mathcal{F}} - 1$$

and with s as in (2) and d_{low} as in Definition 3 the bound $d_{\mathcal{L}(\mathcal{F})} \geq d_{\text{low}}$ follows.

We show the existence of a unique decoder for up to e_{low} errors by proving that in this case $f(\mathbf{a}) = \arg\min_{\alpha \in \mathbb{F}_q}\{N_{\mathbf{a}}(\alpha)\}$ with $N_{\mathbf{a}}(\alpha)$ as in Definition 2.

Suppose that a function $g : \mathbb{F}_Q^m \to \mathbb{F}_q$ is close to some function $f \in \mathcal{L}(\mathcal{F})$ so that $d(f,g) \leq e_{\text{low}}$. For $\alpha = f(\mathbf{a})$, we have $e_{\text{low}} \geq d(f,g) \geq N_{\mathbf{a}}(\alpha)$ by Lemma 2. Assume there exists an $\alpha' \in \mathbb{F}_q$ with $\alpha' \neq \alpha$ and $N_{\mathbf{a}}(\alpha') \leq N_{\mathbf{a}}(\alpha)$. Then

$$N_{\mathbf{a}}(\alpha) + N_{\mathbf{a}}(\alpha') \geq \underbrace{\mathbb{1}\{g^{(V_i)}(\mathbf{a}) \neq \alpha\} + \mathbb{1}\{g^{(V_i)}(\mathbf{a}) \neq \alpha'\}}_{\geq 1}$$

$$+ \sum_{j=0}^{e} \underbrace{(2e + 1)}_{\geq d_{\mathcal{F}} - 1}(M_{\mathbf{a}}(\alpha, j) + M_{\mathbf{a}}(\alpha', j))$$

$$+ \sum_{\beta \neq \alpha, \alpha'} \sum_{j=0}^{e} \underbrace{2(d_{\mathcal{F}} - 1 - j + \delta_{\mathbf{a}}(\beta))}_{\geq d_{\mathcal{F}} - 1} M(\beta, j)$$

$$+ \underbrace{(2e + 2 - \delta_{\mathbf{a}}(\hat{\alpha}) - \delta_{\mathbf{a}}(\hat{\alpha}))}_{\geq d_{\mathcal{F}} - 1} M_{\mathbf{a}}(\star)$$

$$\geq 1 + (d_{\mathcal{F}} - 1)\left(\sum_{\alpha,j} M_{\mathbf{a}}(\alpha, j) + M_{\mathbf{a}}(\star)\right) \overset{(4)}{=} d_{\text{low}} . \quad (6)$$

By Lemma 2 and definition of e_{low} and d_{low}, this is a contradiction and we conclude that $f(\mathbf{a}) = \arg\min_{\alpha \in \mathbb{F}}\{N_{\mathbf{a}}(\alpha)\}$.

To estimate the running time of the described algorithm first note that the values $N_{\mathbf{a}}(\alpha) \ \forall \ \mathbf{a} \in \mathbb{F}_Q^m, \alpha \in \mathbb{F}_q$ can be obtained from the decoding results

- $\mathfrak{D}'(g_{\mathbf{a}}^{(V_i)}(\mathbf{y})) \ \forall \ \mathbf{a} \in \mathbb{F}_Q^m, i \in [s]$ if $d_{\mathcal{F}}$ is odd,
- $\mathfrak{D}'(\tilde{g}_{\mathbf{a}}^{(V_i)}(\mathbf{y})) \ \forall \ \mathbf{a} \in \mathbb{F}_Q^m, i \in [s]$ if $d_{\mathcal{F}}$ is even, where $\tilde{g}_{\mathbf{a}}^{(V_i)}$ is equal to $g_{\mathbf{a}}^{(V_i)}$, except that an erasure is placed at the origin.

Therefore, the required number of instances of the decoder of $\mathfrak{D}'$ is proportional to the number of points $|\mathbb{F}_Q^m|$, the number of vector spaces s in the (partial) spread, and the running time of the decoder $\mathfrak{D}'$. Hence, it can be estimated by $O(Q^{2m-t}T(\mathfrak{D}'))$. When $d_{\mathcal{F}}$ is odd, we have $g_{\mathbf{a}'}^{(V_i)}(\mathbf{y}) = g_{\mathbf{a}}^{(V_i)}(\mathbf{y} + \varphi_{V_i}(\mathbf{a}' - \mathbf{a})) \ \forall \ \mathbf{a}, \mathbf{a}' \in V_i$ and therefore need to run the local decoder $\mathfrak{D}'$ only once per affine subspace, resulting in a running time of $O(Q^{2m-2t}T(\mathfrak{D}'))$. $\square$

Remark 2. *We have two additional comments:*
1) *If a subcode of $\mathcal{L}(\mathcal{F})$ has low rate, then the complexity of its decoding might be reduced. If it is a linear $[n,k]_q$-code, then it can be represented as a systematic code. Thus, it suffices to reconstruct k information symbols and, if necessary, encode them to get the whole codeword. Thus, the running time is $O(knQ^{-t}T(\mathfrak{D}'))$ (plus $O(nk)$ operations for encoding) in this case.*
2) *A randomized local correction algorithm for lifted Reed-Solomon and Reed-Muller codes was proposed in [14]. A key idea of that algorithm is similar to the algorithm of Theorem 1, namely: assign appropriate weights to the results of local decoding and aggregate them to get a final decision for a symbol.*

IV. HIGH-ERROR RANDOMIZED DECODING

In this section, we show that for any fixed linear affine-invariant code $\mathcal{F} \subseteq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$, long lifted codes $\mathcal{L}(\mathcal{F})$ can correct almost all patterns of errors with the relative weight less than $\frac{q-1}{q} - \varepsilon$ with $\varepsilon > 0$. To this end, we introduce the q-ary symmetric channel (q-SC) with error probability $p_{q,\varepsilon} := \frac{q-1}{q} - \varepsilon$ that takes a q-ary symbol at its input and outputs either the unchanged input symbol, with probability $1 - p_{q,\varepsilon}$, or one of the other $q-1$ symbols, with probability $\frac{p_{q,\varepsilon}}{q-1}$. We shall discuss the case when $\mathcal{F}$ is a single parity-check (SPC) code, but the same decoding algorithm works well for any non-trivial affine-invariant code $\mathcal{F} \subsetneq \{\mathbb{F}_Q^t \to \mathbb{F}_q\}$.

Theorem 2. *Suppose that $\mathcal{F} \subseteq \{\mathbb{F}_Q \to \mathbb{F}_q\}$ is a SPC code, i.e., for any $f \in \mathcal{F}$, $\sum_{\mathbf{a} \in \mathbb{F}_Q} f(\mathbf{a}) = 0$. Let $\mathcal{L}(\mathcal{F}) \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$ be a lifted code as in Definition 1.*
1) ***Parameters of the code:** The dimension and the length of the code are*
$$\dim_{\mathbb{F}_q}(\mathcal{L}(\mathcal{F})) = \Theta_Q\left(m^{Q-2}\right), \quad n = Q^m.$$
2) ***High-error randomized decoder:** Let $f \in \mathcal{L}(\mathcal{F})$ and g be a random function each value of which is obtained independently after transmitting the corresponding value of f over the q-SC with error probability $p_{q,\varepsilon}$. For any $\delta > \exp(-cn)$ with some constant $c = c(Q,\varepsilon)$, there exists a decoder $\mathfrak{D}$ running in time $O_Q\left(\frac{\log \frac{1}{\delta} + \log\log n}{\varepsilon^{2Q-2}}\right)$ such that the error probability $\Pr\{\mathfrak{D}(g) \neq f\} < \delta$.*

Proof. The lower bound on the dimension of the code was already proved in [2]. We prove the upper bound in Lemma 4.

Let $f \in \mathcal{L}(\mathcal{F})$ and g be a noisy version of f, where each symbol of f is corrupted by the q-SC with error probability $p_{q,\varepsilon} = \frac{q-1}{q} - \varepsilon$. We fix a partial spread of $\mathbb{F}_Q^m$ into one-dimensional vector subspaces $V_1, \ldots, V_s$, where the number s with $s \leq (q^m - 1)/(q-1)$ will be specified later. For any $i \in [s]$ and $\mathbf{a} \in \mathbb{F}_Q^m$, by the definition of lifting it follows that $f_{\mathbf{a}}^{(V_i)}$ belongs to $\mathcal{F}$. Since $\mathcal{F}$ is a SPC code, the symbol $f(\mathbf{a})$ can be reconstructed by reading symbols indexed by $\mathbf{b} \in \mathbf{a} + V_i \setminus \{\mathbf{a}\}$, i.e.,
$$f(\mathbf{a}) = - \sum_{\mathbf{b} \in \mathbf{a} + V_i \setminus \{\mathbf{a}\}} f(\mathbf{b})$$

Define the indicator random variables
$$\psi_{\mathbf{a}}^{(i)} := \mathbb{1}\left\{-f(\mathbf{a}) = \sum_{\mathbf{b} \in \mathbf{a} + V_i \setminus \{\mathbf{a}\}} g(\mathbf{b})\right\},$$
$$\psi_{\mathbf{a}}^{(i,\alpha)} := \mathbb{1}\left\{-f(\mathbf{a}) = \alpha + \sum_{\mathbf{b} \in \mathbf{a} + V_i \setminus \{\mathbf{a}\}} g(\mathbf{b})\right\} \quad \text{for } \alpha \in \mathbb{F}_q^*.$$

Then, by Lemma 3, the mathematical expectation
$$\mathbb{E}[\psi_{\mathbf{a}}^{(i)}] = \frac{1}{q} + \frac{q-1}{q}\left(\frac{\varepsilon q}{q-1}\right)^{Q-1} =: \hat{p}$$
and for any $\alpha \in \mathbb{F}_q^*$,
$$\mathbb{E}[\psi_{\mathbf{a}}^{(i,\alpha)}] = \frac{1}{q} - \frac{1}{q}\left(\frac{\varepsilon q}{q-1}\right)^{Q-1} =: \check{p}.$$

Then we define the random variables
$$\Sigma_{\mathbf{a}} := \sum_{i \in [s]} \psi_{\mathbf{a}}^{(i)}, \quad \Sigma_{\mathbf{a}}^{(\alpha)} := \sum_{i \in [s]} \psi_{\mathbf{a}}^{(i,\alpha)} \quad \text{for } \alpha \in \mathbb{F}_q^*.$$

Suppose that we do the majority decision for the symbol $f(\mathbf{a})$ by taking $\beta \in \mathbb{F}_q$ that maximizes the number of subspaces $\mathbf{a} + V_i$, for which $\sum_{\mathbf{b} \in \mathbf{a} + V_i \setminus \{\mathbf{a}\}} g(\mathbf{b}) = -\beta$. Then the result of the decoding would be incorrect with probability at most
$$\Pr\left\{\Sigma_{\mathbf{a}} < \Sigma_{\mathbf{a}}^{(\alpha)} \text{ for some } \alpha \in \mathbb{F}_q^*\right\}. \tag{7}$$

Note that $\Sigma_{\mathbf{a}}$ and $\Sigma_{\mathbf{a}}^{(\alpha)}$ are binomial random variables $B(s,\hat{p})$ and $B(s,\check{p})$. Let $\bar{p} := (\hat{p} + \check{p})/2$. Employing Hoeffding's bound, we estimate the probability (7) by
$$(q-1)\left(\Pr\{B(s,\hat{p}) < \bar{p}s\} + \Pr\{B(s,\check{p}) \geq \bar{p}s\}\right)$$
$$\leq 2(q-1)\exp(-2(\hat{p} - \check{p})^2 s)$$

By Lemma 4, $\dim_{\mathbb{F}_q}(\mathcal{L}(\mathcal{F})) = \Theta_Q(m^{Q-2})$. To reconstruct the original polynomial f, it suffices to recover the evaluation of f at information positions only. Thus, by the union bound, the probability of error in recovering information symbols can be bounded by $O_Q\left(m^{Q-2}\exp(-2(\hat{p} - \check{p})^2 s)\right)$. This value is less than δ, if $s = \Omega_Q\left(\frac{\log\frac{1}{\delta} + \log m}{\varepsilon^{2Q-2}}\right)$. $\square$

Lemma 3. *Let $\xi_1, \ldots, \xi_k$ be i.i.d. random variables taking the value 0 with probability $1 - \varepsilon$ and any other value in the field $\mathbb{F}_q$ with probability $\frac{\varepsilon}{q-1}$. Then*
$$\Pr\left\{\sum_{i=1}^k \xi_i = 0\right\} = \frac{1}{q} + \left(1 - \frac{1}{q}\right)\left(1 - \frac{q\varepsilon}{q-1}\right)^k$$

and for any $\alpha \in \mathbb{F}_q^*$,

$$\Pr\left\{\sum_{i=1}^{k} \xi_i = \alpha\right\} = \frac{1}{q} - \frac{1}{q}\left(1 - \frac{q\varepsilon}{q-1}\right)^k$$

Proof. We shall prove this statement by induction on k. For $k = 1$, the statement is trivial. Suppose that the statement holds for $k - 1$. From the independence of the variables ξ_i and the inductive assumption, it follows that

$$\Pr\left\{\sum_{i=1}^{k} \xi_i = 0\right\} = \sum_{\beta \in \mathbb{F}_q} \Pr\left\{\sum_{i=1}^{k-1} \xi_i = -\beta, \ \xi_k = \beta\right\}$$

$$= \sum_{\beta \in \mathbb{F}_q} \Pr\left\{\sum_{i=1}^{k-1} \xi_i = -\beta\right\} \Pr\{\xi_k = \beta\}$$

$$= \left(\frac{1}{q} + \left(1 - \frac{1}{q}\right)\left(1 - \frac{q\varepsilon}{q-1}\right)^{k-1}\right)(1 - \varepsilon)$$

$$+ \left(\frac{1}{q} - \frac{1}{q}\left(1 - \frac{q\varepsilon}{q-1}\right)^{k-1}\right)\varepsilon$$

$$= \frac{1}{q} + \left(1 - \frac{q\varepsilon}{q-1}\right)^{k-1}\left(\frac{(q-1)(1-\varepsilon)}{q} - \frac{\varepsilon}{q}\right)$$

$$= \frac{1}{q} + \left(1 - \frac{1}{q}\right)\left(1 - \frac{q\varepsilon}{q-1}\right)^k.$$

Clearly, $\Pr\left\{\sum_{i=1}^{k} \xi_i = \alpha\right\}$ doesn't depend on $\alpha \in \mathbb{F}_q^*$. Thus,

$$\Pr\left\{\sum_{i=1}^{k} \xi_i = \alpha\right\} = \frac{1 - \Pr\left\{\sum_{i=1}^{k} \xi_i = 0\right\}}{q - 1}$$

$$= \frac{1}{q} - \frac{1}{q}\left(1 - \frac{q\varepsilon}{q-1}\right)^k.$$

$\square$

Lemma 4. *Suppose that $\mathcal{F} \subseteq \{\mathbb{F}_Q \to \mathbb{F}_q\}$ is a SPC code. Let $\mathcal{L}(\mathcal{F}) \subseteq \{\mathbb{F}_Q^m \to \mathbb{F}_q\}$ be a lifted code as in Definition 1. Then the dimension of the code $\mathcal{L}(\mathcal{F})$ is $\Theta_Q(m^{Q-2})$.*

Proof. First we introduce some useful notation. Recall that $q = p^l$ for a prime integer p. A tuple $\mathbf{c} \in \mathbb{Z}_q^m$ is less than or equal to a tuple $\mathbf{d} \in \mathbb{Z}_q^m$ by the *p-partial order*, say $\mathbf{c} \leq_p \mathbf{d}$, if $c_i = \sum_{j=0}^{l-1} c_i^{(j)} p^j$ and $d_i = \sum_{j=0}^{l-1} d_i^{(j)} p^j$ and $c_i^{(j)} \leq d_i^{(j)}$ for all $i \in [m]$ and $j \in \mathbb{Z}_l$. Define an operation $\pmod^* q$ that takes a non-negative integer and maps it to the element from $\mathbb{Z}_q$ as follows

$$a \pmod^* q := \begin{cases} 0, & \text{if } a = 0, \\ b \in [q-1], & \text{if } a \neq 0, \ a = b \pmod{q-1}. \end{cases}$$

For a tuple $\mathbf{d}$, we also define its *degree* $\deg(\mathbf{d})$ to be $\sum_{i=1}^{m} d_i$.

In [2], it was proved that $\dim_{\mathbb{F}_q}(\mathcal{L}(\mathcal{F}))$ can be found by counting all possible *good* tuples $\mathbf{d} \in \mathbb{Z}_Q^m$ such that there is no $\mathbf{c} \in \mathbb{Z}_Q^m$ such that $\mathbf{c} \leq_p \mathbf{d}$ and $\deg(\mathbf{c}) \pmod^* Q) = Q - 1$. Let $S \subset [m]$ with $|S| = Q - 2$ and a tuple $\mathbf{d} = \mathbf{d}(S) \in \mathbb{Z}_Q^m$ has the property $d_i = 1$ for $i \in S$ and $d_i = 0$ otherwise. Clearly, all $\binom{m}{Q-2}$ such tuples are good. Thus, $\dim_{\mathbb{F}_q}(\mathcal{L}(\mathcal{F})) \geq \Omega_Q(m^{Q-2})$ which was first shown in [2].

It remains to prove the upper bound on the dimension. We shall prove that the number of appropriate $\mathbf{d} \in \mathbb{Z}_Q^m$ is at most $\left(1 + \log_p Q^m\right)^{Q-2}$. Toward a contradiction, assume that it is larger than this value. Then, there exists at least one $\mathbf{d}$ such that $\sum_{i=1}^{m} \sum_{j=0}^{\log_p Q - 1} d_i^{(j)} \geq Q - 1$. We will prove that this $\mathbf{d}$ cannot be good, i.e., there exists a $\mathbf{c} \in \mathbb{Z}_Q^m$ with $\mathbf{c} \leq_p \mathbf{d}$ such that $\deg(\mathbf{c}) \pmod^* Q) = Q - 1$. To see this, we construct a sequence of $Q - 1$ distinct tuples $\mathbf{c}_1, \ldots, \mathbf{c}_{Q-1} \in \mathbb{Z}_Q^m$ with positive degrees such that $\mathbf{c}_{i-1} \leq_p \mathbf{c}_i \leq_p \mathbf{d}$ for $i \in [Q-1]$. Clearly, if all $\deg(\mathbf{c}_i) \pmod^* Q)$ are different, then there exists $j \in [Q-1]$ so that $\deg(\mathbf{c}_j) \pmod^* Q) = Q - 1$. On the other hand, if $\deg(\mathbf{c}_i) \pmod^* Q) = \deg(\mathbf{c}_j) \pmod^* Q)$ for $i < j$, then the tuple $\mathbf{c} := \mathbf{c}_j - \mathbf{c}_i \neq \mathbf{0}$ satisfies two required conditions: $\deg(\mathbf{c}) \pmod^* Q) = Q - 1$ and $\mathbf{c} \leq_p \mathbf{c}_j \leq_p \mathbf{d}$. Thus, $\mathbf{d}$ is not good and this contradiction completes the proof. $\square$

REFERENCES

[1] F. J. MacWilliams and N. J. A. Sloane, *The theory of error correcting codes*. Elsevier, 1977, vol. 16.

[2] A. Guo, S. Kopparty, and M. Sudan, "New affine-invariant codes from lifting," in *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*, 2013, pp. 529–540.

[3] L. Holzbaur, R. Polyanskaya, N. Polyanskii, and I. Vorobyev, "Lifted reed-solomon codes with application to batch codes," in *2020 IEEE Int. Symp. Inf. Theory (ISIT)*, 2020, pp. 634–639.

[4] S. Arora and M. Sudan, "Improved low-degree testing and its applications," *Combinatorica*, vol. 23, no. 3, pp. 365–426, 2003.

[5] O. Goldreich, R. Rubinfeld, and M. Sudan, "Learning polynomials with queries: The highly noisy case," *SIAM Journal on Discrete Mathematics*, vol. 13, no. 4, pp. 535–570, 2000.

[6] M. Sudan, L. Trevisan, and S. Vadhan, "Pseudorandom generators without the XOR lemma," *Journal of Computer and System Sciences*, vol. 62, no. 2, pp. 236–266, 2001.

[7] I. Dumer, "Recursive decoding and its performance for low-rate Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 5, pp. 811–823, 2004.

[8] R. Krichevskiy, "On the number of Reed-Muller code correctable errors," in *Dokl. Sov. Acad. Sci*, vol. 191, 1970, pp. 541–547.

[9] P. Delsarte, J.-M. Goethals, and F. J. Mac Williams, "On generalized Reed-Muller codes and their relatives," *Information and Control*, vol. 16, no. 5, pp. 403–442, 1970.

[10] T. Kasami, S. Lin, and W. Peterson, "New generalizations of the Reed-Muller codes–I: Primitive codes," *IEEE Trans. Inf. Theory*, vol. 14, no. 2, pp. 189–199, 1968.

[11] J. L. Massey, D. J. Costello, and J. Justesen, "Polynomial weights and code constructions," *IEEE Trans. Inf. Theory*, vol. 19, no. 1, pp. 101–110, 1973.

[12] R. Pellikaan and X.-W. Wu, "List decoding of q-ary Reed-Muller codes," *IEEE Trans. Inf. Theory*, vol. 50, no. 4, pp. 679–682, 2004.

[13] J. Y. Kim and S. Kopparty, "Decoding Reed-Muller codes over product sets," in *31st Conference on Computational Complexity*, 2016.

[14] A. Guo and S. Kopparty, "List-decoding algorithms for lifted codes," *IEEE Trans. Inf. Theory*, vol. 62, no. 5, pp. 2719–2725, 2016.

[15] S. Gao, "A new algorithm for decoding Reed-Solomon codes," in *Communications, Information and Network Security*. Springer, 2003, pp. 55–68.

[16] T. Kaufman and M. Sudan, "Algebraic property testing: the role of invariance," in *Proceedings of the fortieth annual ACM symposium on Theory of computing*, 2008, pp. 403–412.

[17] E. Ben-Sasson, E. Grigorescu, G. Maatouk, A. Shpilka, and M. Sudan, "On sums of locally testable affine invariant properties," in *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques*. Springer, 2011, pp. 400–411.

[18] T. Bu, "Partitions of a vector space," *Discrete Mathematics*, vol. 31, no. 1, pp. 79–83, 1980.