Electronic Colloquium on Computational Complexity, Report No. 154 (2011)

From Irreducible Representations to Locally Decodable Codes

Klim Efremenko*

November 1, 2011

Abstract

Locally Decodable Code (LDC) is a code that encodes a message in a way that one can decode any particular symbol of the message by reading only a constant number of locations, even if a constant fraction of the encoded message is adversarially corrupted.

In this paper we present a new approach for the construction of LDCs. We show that if there exists an irreducible representation (ρ, V) of G and q elements $g_1, g_2, \ldots, g_q$ in G such that there exists a linear combination of matrices $\rho(g_i)$ that is of rank one, then we can construct a q-query Locally Decodable Code $\mathcal{C} : V \to \mathbb{F}^G$.

We show the potential of this approach by constructing constant query LDCs of sub-exponential length matching the parameters of the best known constructions.

1 Introduction

A *Locally Decodable Codes (LDC)* is a code that allows the retrieval of any symbol of a message by reading only a constant number of symbols from its codeword, even if a large fraction of the codeword is adversarially corrupted. Formally, a code $\mathcal{C}$ is said to be locally decodable with parameters (q, δ, ϵ) if for all message x and for all indices i it is possible to recover any symbol x_i of a message x by making at most q queries to $\mathcal{C}(x)$, such that even if a δ fraction of $\mathcal{C}(x)$ is adversarially corrupted, the decoding algorithm returns the correct answer with probability at least $1 - \epsilon$.

Local decoding is an important concept in theoretical computer science and cryptography. Many important results in these fields use such codes in different variations. LDCs are closely related to such subjects as worst case – average case reductions, pseudo-random generators, hardness amplification, private information retrieval schemes and many others. See the surveys [Tre04, Gas04] for more details.

*The Blavatnik School of Computer Science, Tel-Aviv University, Israel, 69978. Supported by the Adams Fellowship Program of the Israel Academy of Sciences and Humanities, by the Israel Science Foundation klimefrem@gmail.com.

ISSN 1433-8092

Locally decodable codes were first formally defined by Katz and Trevisan [KT00], although this notion already appeared implicitly in previous works. When the number of queries is $poly \log k$, where k is the length of the message, Reed-Muller codes give polynomial length LDCs. When the number of queries is k^{ε}, a variant of Reed-Muller [KSY11] gives LDCs of rate approaching one. For more details on recent results on LDCs see the survey by Yekhanin [Yek10].

The main focus of this paper is LDCs with a constant number of queries. The Hadamard code is the best-known 2-query LDC and is of length 2^k. Tight lower bound of $2^{\Theta(k)}$ on the length of *linear* 2-query locally decodable codes were given in Goldreich et al. [GKST02], and were extended to general codes by Kerenidis and de Wolf [KdW03]. When the number of queries is constant and greater than two, much less is known. For an arbitrary constant number of queries q, only weak super-linear lower bounds are known, see [KT00, KdW03, Woo07]. For many years it was conjectured that LDCs should have an exponential dependence on k for any constant number of queries, until Yekhanin's breakthrough [Yek08]. Yekhanin obtained 3-query LDCs with sub-exponential length under a highly believable conjecture. Later on in [Efr09] this construction was generalized and the dependence on the conjecture was removed. We are still very far from understanding what are the best parameters of LDCs. For example, the best upper bound on three query LDCs is

$$\exp(\exp(\sqrt{\log k \log\log k})),$$

where k is message length in contrast to $\tilde{\Omega}(k^2)$ lower bound. No better lower bounds are known, even for some very restricted special cases of LDCs.

Today all known sub-exponential constructions of LDCs with constant number of queries could be described in the framework of *matching vector codes* (MVCs), which are based on two ingredients: a set of *matching vectors* (MV) and a *decoding polynomial*.(See [Efr09], where this was made explicit.) Some progress was obtained recently in understanding the latter component [IS08, MFL$^+$10], but it seems that in order to make a significant improvement in MVCs, we need to improve also matching vectors, where there was almost no progress in the last ten years. We say that $\{u_i\}_{i=1}^k \subset \mathbb{Z}_m^h$ are S-Matching Vectors (MV), where S is a subset of $\mathbb{Z}_m$ if $\langle u_i, u_j \rangle \in S \Leftrightarrow i \neq j$. The history of Matching Vectors is similar to the history of LDCs. It was conjectured for many years that there must be a polynomial upper bound on the size of MV, until Grolmusz's [Gro00] breakthrough. This construction is the basis for subexponential constructions of LDCs in [Efr09]. For MVs as well, there is not even a conjecture today of what are their best possible parameters.

Although the framework of MVCs is pretty simple it still does not explain the real nature of LDCs. This leads us to seek a new approach to understanding LDCs. In this paper we start a systematic study of LDCs from the point of view of the representation theory. We present a new framework for the construction of LDCs and show that it captures two important classes of LDCs: Reed Muller codes and MVCs. We believe that this is the real algebraic nature behind LDCs.

1.1 Our Results

Let G be a finite group. A *representation* of the group G is a pair (ρ, V) of a vector space V and a mapping $\rho : G \to GL(V)$ from G to the group of invertible matrices over V which is a group

homomorphism, i.e., for all $g_1, g_2 \in G$ it holds that $\rho(g_1 g_2) = \rho(g_1)\rho(g_2)$. A subspace $W \subset V$ is a *sub-representation* of (ρ, V) if for every $g \in G$ the matrix $\rho(g)$ maps W to W. A representation is called *irreducible* if it does not have any non-trivial sub-representations. (See Section 2.1.2 for formal definitions.)

In this paper we study the connection between the representations of finite groups and LDCs. We show that if (ρ, V) is an irreducible representation and there exists a small number of elements $g_1, \ldots, g_q$ in G such that some linear combination of $\rho(g_i)$ is a rank one matrix, then we can construct a q-query LDC of length $|G|$ and dimension $\dim V$.[1]

Theorem 1.1. *(Informal) Let G be a finite group and let (ρ, V) be an irreducible representation of G with $g_1, \ldots, g_q$ in G and $c_1, \ldots c_q \in \mathbb{F}$ such that $\mathrm{Rank}(\sum c_i \rho(g_i)) = 1$. Then there exists a $(q, \delta, q\delta)$-locally decodable code $\mathcal{C} : V \to \mathbb{F}^G$.*

This gives a completely new approach to constructing LDCs. Now in order to construct an LDC it is enough to construct irreducible representations with a sparse element of the group algebra of rank one. This theorem gives what we believe is the real algebraic nature behind LDCs.

Given this, we ask a natural question: When can one construct such a representation? We show that in this framework we can achieve the parameters of the best known construction. The code that we get is the same as in [Efr09].

On the connection between Matching Vectors and our approach: The question when do MV codes fall in the framework of irreducible representations is completely not obvious. We say that MV are *symmetric* if they are an orbit of some group acting on $\mathbb{Z}_m^h$. We show in Section 4 that MV Codes can be explained in the framework of irreducible representations for MV that are symmetric. Next we show that the construction given in [Gro00] is symmetric.[2] This gives a way to interpret the construction in [Efr09] as a construction of an irreducible representation. The relationship between MV and LDCs is summarized in the following diagram:

$$\begin{array}{ccc} \text{Irreducible Representation} & \Rightarrow & \text{LDC} \\ \Uparrow & & \Uparrow \\ \text{Symmetric MV} & \Rightarrow & \text{MV} \end{array}$$

Modular Representations and Reed-Muller Codes: One might wonder if the requirement on the representation being irreducible is essential. Perhaps better locally decodable codes can be constructed with reducible representations? We deal with this question in Section 6. We distinguish two cases. The first is when the characteristic of the field does not divide the size of the group. In this case we show that irreducibility is essential for our construction to lead to locally decodable codes. The second case is when the characteristic of the field divides the size of the group; this brings us to a slightly less familiar territory of representation theory known as *modular representation theory*. We show that in this case, it *is* possible to construct locally decodable codes based

[1] In fact we prove a stronger statement. For details see Theorem 3.1.

[2] In fact, for sake of simplicity, we show it only for a slight modification of Grolmusz [Gro00] construction. While it is true for the Grolmusz construction as well.

on reducible representations. We still don't know, unfortunately, if this can lead to improvements over the best known constructions of LDCs, although this is definitely a promising direction. We illustrate this case by showing how one can view Reed-Muller codes as a special case of our result for reducible modular representations.

Future Research Our main open question is, of course, to construct a *sparse* element of the group algebra that acts as a *rank one* element on a large irreducible representation. Rank one elements arise naturally in representation theory and have been investigated extensively before. Unfortunately, the sparseness property is hard to capture with existing algebraic tools. We hope that this paper will provide motivation to the study of sparse elements in the group algebra.

1.2 Organization of the paper

In Section 2 we give basic definitions and facts about representations of finite groups and LDCs. Section 3 is the main section of this paper where we prove that irreducible representations with a sparse element of rank one imply LDCs. Next we show the connection between the MV Codes construction and the irreducible representations with a sparse element. In order to do so, we present the construction given in [Efr09] in a different way. In Section 4 we show that a Symmetric MV imply irreducible representations with a sparse element of rank one. In Section 5 we show that a variant of Grolmusz [Gro00] gives a Symmetric MV with essentially the same parameters. In Section 6 we generalize Theorem 1.1 to *reducible* representations and we show that this generalizations is useful only for modular representations. We show that Reed-Muller code is an example of an LDC from the such representations. A reader who is not familiar with representation theory may want read first Appendix A were we explain the connection between G-invariant codes and representations of G.

2 Notation and Preliminaries

2.1 Representation Theory

In this section we give basic facts about representation theory. We do not give proofs here and the interested reader is referred to any standard textbook on the subject such as [Ser77].

2.1.1 Group Action

First let us start with the definition of the action of a group on a set.

Definition 2.1. *We say that a group G acts on a set X if there exists a mapping $T : G \times X \to X$ such that $T(g_2, T(g_1, x)) = T(g_2 g_1, x)$ and $T(1, x) = x$.*

Usually the action is obvious from the context and then we write $g \cdot x$ instead of $T(g, x)$. Note that each $g \in G$ defines a permutation on the set X.

Definition 2.2. *We say that G acts transitively on the set X iff for every $x, y \in X$ there exists $g \in G$ such that $gx = y$. In this case we say that X is an orbit of G.*

Let us assume that G acts on the set X. Then using this action we can define a new action of the group G on Σ^X. It is more convenient to view Σ^X as the set of functions from X to Σ rather than a string of symbols, i.e., we view $f \in \Sigma^X$ as $f : X \to \Sigma$.

Definition 2.3. *Suppose G acts on the set X. Define an action of G on Σ^X by $(gf)(x) = f(g^{-1}x)$. We call such an action a permutation action.*

Note that we need to prove that this is indeed an action. That is, we need to check that $(g_1 \cdot (g_2 \cdot f)) = (g_1 \cdot g_2) \cdot f$. Note also that if we view Σ^X as a set of strings, then G acts on it by permuting coordinates.

Definition 2.4. *An* order *of the group G is a minimal number m such that for every $g \in G$ it holds that $g^m = 1$.*

Definition 2.5. *We say that the group H* acts on the group *N if it acts on it as a set and for every $h \in H, n_1, n_2 \in N$ it holds that*

$$h \cdot (n_1 n_2) = (h \cdot n_1)(h \cdot n_2) \ . \tag{2.1}$$

Any group N has a natural action on the set N. Note that this action does not satisfies the Equation 2.1.

Definition 2.6 (Semi-Direct Product of Groups)**.** *Let N be a group. Let H be a group acting on the group N. Then the semi-direct product of N by H denoted by $N \rtimes H$ is a sub-group of permutations of N. Generated by the permutations defined by the actions of N and H on the set N.*

2.1.2 Group Representations

Notation 2.1. *We denote by $\mathrm{Mat}(V)$ the set of all matrices on the vector space V. $GL(V)$ denotes the group of invertible matrices on the vector space V.*

Definition 2.7 (Representation of a Group)**.** *A representation (ρ, V) of a group G in a vector space V is a group homomorphism $\rho : G \to GL(V)$, that is, for every $g_1, g_2 \in G$ it holds that $\rho(g_1) \cdot \rho(g_2) = \rho(g_1 \cdot g_2)$.*

We also can define a representation of group G as an action of G on vector space as follows:

Definition 2.8. *Let V be a vector space over the field $\mathbb{F}$. A representation of a group G in V is an action of the group G on the set V which satisfies the following conditions:*

- *For any $v_1, v_2 \in V$ it holds that $g \cdot (v_1 + v_2) = g \cdot v_1 + g \cdot v_2$.*
- *For any $\lambda \in \mathbb{F}$ it holds that $g \cdot (\lambda v) = \lambda g \cdot v$.*

- *For any $v \in V$ it holds that $1 \cdot v = v$.*

Definition 2.9 (Sub-Representation)**.** *Let ρ be a representation of a group G in a vector space V. We say that $U \subset V$ is a sub-representation of ρ if U is a linear subspace of V and U is invariant under ρ, namely: for every $g \in G$ it holds that $\rho(g)U = U$.*

Definition 2.10 (Irreducible-Representation)**.** *Let ρ be a representation of a group G in a vector space V. We say that ρ is an irreducible representation if it does not have any non trivial sub-representations, else we say that ρ is reducible.*

We need the following decomposition theorem:

Theorem 2.2 (Complete Reducibility)**.** *Let G be a group. Let V be a vector space over an algebraically closed field $\mathbb{F}$ of characteristic co-prime to the size of G. Let ρ be a representation of the G in the vector space V. Then $V = \oplus V_i$ where V_i are irreducible sub-representations of ρ.*

The following theorem says that any orbit of an irreducible representation spans the entire space.

Lemma 2.3. *Let (ρ, V) be an irreducible representation of G. Let $v \in V$ be a non-zero vector. Then the set $\{\rho(g)v | g \in G\}$ spans V, and thus there exist $g_1, g_2, \ldots, g_k \in G$ such that $\{\rho(g_i)v\}_{i=1}^k$ is a basis for V.*

2.1.3 Homomorphisms between Representations

Definition 2.11. *Let ρ_1 be a representation of the group G in a vector space V and ρ_2 be a representation of the group G in a vector space W. We say that a linear mapping $T : V \to W$ is a homomorphism from (ρ_1, V) to (ρ_2, W) iff $\forall g \in G\ \rho_2(g) \circ T = T \circ \rho_1(g)$. Sometimes we also say that T is a G-homomorphism.*

Schematically a linear mapping T is a homomorphism between (ρ_1, V) and (ρ_2, W) if the following diagram is commutative:

$$\begin{array}{ccc} V & \xrightarrow{T} & W \\ \rho_1(g) \downarrow & & \downarrow \rho_2(g) \\ V & \xrightarrow{T} & W \end{array}$$

We say that a homomorphism T from (ρ_1, V) to (ρ_2, W) is an embedding/isomorphism if T is an embedding/isomorphism of the vector spaces V and W. Note also that kernel of T is a sub-representation. Thus if (ρ_1, V) is irreducible then T is either embedding or zero homomorphism.

Lemma 2.4. *Let (ρ, V) be a representation of G. Let $\{V_i\}_{i=1}^k$ be irreducible non-isomorphic sub-representations of V. Then vector spaces $\{V_i\}_{i=1}^k$ are linearly independent.*

2.1.4 Permutational Representation, Group Algebra

Assume that a group G acts on a set X. Consider the permutation action of G on $\mathbb{F}^X$. It is easy to see that this action admits the properties of Definition 2.8 . Thus we can define a representation τ of the group G in $\mathbb{F}^X$. We call τ the *permutational representation*. Specifically:

$$(\tau(g) \cdot f)(x) = f(g^{-1}x). \tag{2.2}$$

For any $f \in \mathbb{F}^X$ we define support of f by the number of non-zero entries of $f : X \to \mathbb{F}$ i.e.,

$$\text{supp}(f) = |\{x \in X | f(x) \neq 0\}| .$$

For linear subspace $U \subset F^X$, we define support as a union of supports of all vectors in U, i.e.,

$$\text{supp}(U) = |\cup_{f \in U} \{x \in X | f(x) \neq 0\}| \ .$$

Lemma 2.5. *Let U be a vector subspace of $\mathbb{F}^X$ of the full support and let $|\mathbb{F}| \geq t$. Then there exist a vector $u \in U$ such that supp$(u) \geq (1 - \frac{1}{t})|X|$.*

Now let us define the group algebra $\mathbb{F}[G]$:

Definition 2.12 (Group Algebra)**.** *The group algebra $\mathbb{F}[G]$ is the set of all functions from G to $\mathbb{F}$. Multiplication in this group algebra is given by*

$$(f * h)(x) = \sum_{g_1 \cdot g_2 = x} f(g_1)h(g_2) .$$

We write $f \in \mathbb{F}[G]$ as a formal sum: $f = \sum_{i=1}^{n} a_i g_i$ meaning that $f(g_i) = a_i$ for $g_1, g_2, \ldots, g_n$ and zero on the rest of G. We say that $f \in \mathbb{F}[G]$ is a q-sparse element if it has support of size at most q i.e., it can be written in the form $f = \sum_{i=1}^{q} a_i g_i$.

Definition 2.13 (Regular Representation)**.** *The regular representation of the group G is the representation ρ in the group algebra $\mathbb{F}[G]$ given by: $\rho(g)f = g * f$.*

Note that an equivalent way to define the regular representation is as a permutational representation of $\mathbb{F}^G$, where the group G acts on G in a natural way.

The regular representation plays an important role since it contains all irreducible representations. It follows from the following basic theorem from representation theory.

Theorem 2.6. *Let V be a vector space over the field $\mathbb{F}$. Then for every irreducible representation (ρ, V) there exists some G-embedding from V to $\mathbb{F}[G]$.*

Notation 2.7. *Let $\rho : G \to GL(V)$ be any representation of the group G. Then we can linearly extend ρ to the group algebra $\mathbb{F}[G]$ i.e., $\rho : \mathbb{F}[G] \to \text{Mat}(V)$ where $\rho(f)$ is defined as $\sum_{g \in G} f(g)\rho(g)$. Note that now $\rho(f)$ may be any matrix, not necessary invertible.*

Note that if $(\rho_1, V), (\rho_2, W)$ are two representations and $T : V \to W$ is a homomorphism between them, then for any $f \in \mathbb{F}[G]$ it holds that

$$T \circ \rho_1(f) = \rho_2(f) \circ T. \tag{2.3}$$

2.1.5 Dual Space, Dual Representation

Definition 2.14. *Let V be a linear vector space over field $\mathbb{F}$. Then the* dual space *of V, denoted by V^* is the set of all linear functionals from V to $\mathbb{F}$.*

We want to mention here that $\dim V = \dim V^*$.

Definition 2.15. *Let V be a vector space of dimension k. Let $u_1, u_2, \ldots, u_k$ be a basis of V and $v_1, \ldots, v_k$ be a basis of V^*. We say these bases are* dual *if $v_i(u_j) = \delta_{i,j}$, where δ_{ij} is Kronecker delta i.e., $\delta_{ij} = 1$ is iff $i = j$ and zero otherwise.*

Theorem 2.8. *For every basis there exists a dual basis.*

Now let us define the dual representation:

Definition 2.16 (Dual Representation)**.** *Let V be a vector space over $\mathbb{F}$. Let (ρ, V) be a representation of the group G. Let V^* be the set of all linear functionals from V to $\mathbb{F}$. The dual representation $(\bar{\rho}, V^*)$ is given by $\bar{\rho}(g)(\ell) = \ell \circ \rho(g^{-1})$, i.e., $\bar{\rho}(g)(\ell)(v) = \ell(\rho(g^{-1})v)$.*

Note that $\dim V = \dim V^*$. Also it holds that $(V^*)^* = V$. We leave to the reader to check that this is indeed a representation. In many cases a representation is isomorphic to its dual representation, but not always. However, a representation is irreducible if and only if its dual is irreducible.

Theorem 2.9. *The representation (ρ, V) is irreducible if and only if $(\bar{\rho}, V^*)$ is irreducible.*

The dual group for Abelian groups is very similar to dual representation.

Definition 2.17. *Let A be an Abelian group. Let m be an order of A. A dual group A^* is a set of group homomorphisms $\theta : A \to \mathbb{Z}_m$.*

Note that if θ_1, θ_2 are group homomorphisms then $\theta_1 + \theta_2$ is also group homomorphism. Therefore, A^* is an Abelian group. Moreover A^* isomorphic to A. For example if $A = \mathbb{Z}_m^h$ then isomorphism is given by $a \mapsto \langle -, a \rangle$. If some group H acts on an Abelian group A then it also acts on its dual A^*. For $h \in H$ and $\theta \in A^*$ the action of is given by the rule $h \cdot \theta(x) = \theta(h^{-1} \cdot x)$.

2.2 Locally Decodable Codes

Definition 2.18. *A code $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^n$ is said to be (q, δ, ε) locally decodable if there exists a randomized decoding algorithm D^w with an oracle access to the received word w such that the following holds:*

1. *For every message $m = (m_1, m_2, \ldots, m_k) \in \mathbb{F}^k$ and for every $w \in \mathbb{F}^n$ such that $\Delta(\mathcal{C}(m), w) \leq \delta n$ for every i, it holds that $\Pr(D^w(i) = m_i) \geq 1 - \varepsilon$, where probability is taken over internal randomness of D. This means that the decoding algorithm can recover the relevant symbol even if up to δ fraction of the codeword symbols are corrupted.*

2. *The algorithm $D^w(i)$ makes at most q queries to w.*

A code $\mathcal{C}$ is called linear if $\mathcal{C}$ is a linear transformation over $\mathbb{F}$. A locally decodable code is called non-adaptive if D makes all its queries simultaneously. Our constructions of locally decodable codes are linear and non-adaptive.

Definition 2.19. *A code $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^n$ is said to have a* c-smooth decoder *if $D^{\mathcal{C}(m)}(i) = m_i$ for every $m \in \mathbb{F}^k$ and for every i. Each query of $D(i)$ is uniformly distributed over a domain of size cn.*

Fact 2.10 (from [Tre04])**.** *Any code with a c-smooth decoder which makes q queries is also $(q, \delta, \frac{q\delta}{c})$ locally decodable.*

Proof. Note that if the decoding algorithm D queries w in uncorrupted places then D outputs the correct answer. The probability that any specific query will be corrupted is at most $\frac{\delta}{c}$. By a union bound, the probability that some query will be corrupted is at most $\frac{q\delta}{c}$. Therefore, the decoder outputs the correct answer with probability at least $1 - \frac{q\delta}{c}$. □

3 Locally Decodable Codes from Irreducible Representations

Let us start from the main theorem of this paper.

Theorem 3.1. *Let G be a group acting on a set X. Let $(\tau, \mathbb{F}^X)$ be the permutational representation defined by this action. Let (ρ, V) be a representation of G. Let $\mathcal{C} : V \to \mathbb{F}^X$ be a G-homomorphism between representations (ρ, V) and $(\tau, \mathbb{F}^X)$. Assume that the following conditions hold:*

1. *(a) There exists a q-sparse element $D \in \mathbb{F}[G],\ D = \sum_{i=1}^{q} c_i g_i$ such that $\mathrm{Rank}(\rho(D)) = 1$.*
   (b) (ρ, V) is an irreducible representation.
2. *Let $v \in \mathrm{Im}(\rho(D))$ be a non-zero vector.*[3] *Then supp$(C(v)) \geq c|X|$.*

Let $k = \dim V$. Then there exists a basis $b_1, \ldots, b_k$ for V such that

$$(m_1, m_2, \ldots, m_k) \mapsto \mathcal{C}(\sum_{i=1}^{k}(m_i b_i))$$

is a $(q, \delta, \frac{q\delta}{c})$-Locally Decodable Code.

In Subsection 3.2 we show that if one constructs a representation ρ that satisfies Condition 1 of Theorem 3.1, then we can always embed it into the regular representation in a way that satisfies Condition 2 of the theorem. In Subsection 3.3 we show that if $\mathbb{F}$ is an algebraic extension of $\mathbb{F}_p$, we can reduce the alphabet to $\mathbb{F}_p$ almost at no cost. In Section 6 we show that when $|\mathbb{F}|$ and $|G|$ are co-prime then the irreducibility of (ρ, V) is essential for having a rank one element. Moreover, we show that (ρ, V) should be irreducible not only over $\mathbb{F}$ but also over the algebraic closure of $\mathbb{F}$.

[3] Note that since $\mathrm{Rank}(\rho(D)) = 1$, the vector v is unique up to scalar multiplication.

Proof. The proof is divided into two parts. The first part is Lemma 3.2 which constructs a basis for V. This basis defines the encoding algorithm. In the second part we construct a decoding algorithm with q queries and show that it is a c-smooth decoder.

Lemma 3.2. *There exists a basis* $\{b_1, b_2, \ldots, b_k\}$ *for* V *and* $h_i, \ldots, h_k \in G$ *such that* $b_i \in \mathrm{Ker}(\rho(D * h_j))$ *if and only if* $i \neq j$.

Proof. Set $L = \mathrm{Ker}\,\rho(D)$. L is a linear subspace of V of dimension $k-1$. Therefore, there exists unique (up to scalar multiplication) non-zero linear functional $u \in V^*$ such that $u(L) = 0$. Since (ρ, V) is an irreducible representation, it follows by Theorem 2.9 that its dual $(\bar{\rho}, V^*)$ is also irreducible. Therefore, from Lemma 2.3[4] it follows that there exist $h_1^{-1}, h_2^{-1}, \ldots, h_k^{-1} \in G$ such that $\{\bar{\rho}(h_i^{-1})u\}_{i=1}^k$ is a basis for V^*. By Theorem 2.8 it follows that for this basis there exists a dual basis $\{b_1, b_2, \ldots, b_k\}$ for V. From the definition of the dual basis it holds that $(\bar{\rho}(h_i^{-1})u)(b_j) = \delta_{ij}$. Thus $b_i \in \mathrm{Ker}\,\bar{\rho}(h_i^{-1})u$ if and only if $i \neq j$. In order to complete the proof of the lemma we need to show that $\mathrm{Ker}(\bar{\rho}(h_i^{-1})u) = \mathrm{Ker}\,\rho(D * h_i)$. Let $v \in \mathrm{Ker}\,\rho(D * h_i)$ then $0 = \rho(D * h_i)v = \rho(D)\rho(h_i)v$. Thus $\rho(h_i)v \in \mathrm{Ker}\,\rho(D)$ by definition of u it also holds that $u(\rho(h_i)v) = 0$. Therefore $\bar{\rho}(h_i^{-1})u(v) = 0$. □

Let $b_1, \ldots, b_k$ and $h_1, \ldots, h_k$ be given by Lemma 3.2. The encoding $\mathcal{C}$ of our Locally Decodable Code encodes a message $m = (m_1, \ldots, m_k)$ by

$$m \mapsto \mathcal{C}(\sum_{i=1}^{k} m_i b_i)\ .$$

In order to prove Theorem 3.1 we show that the following algorithm is a c-smooth decoder (see Definition 2.19).

> **Input:** An oracle access to $w \in \mathbb{F}^X$ and an index $i \in \{1, \ldots, k\}$. Let $D_i = D * h_i = \sum_{j=1}^{q} c_j \cdot g_j h_i$.

1. Set $y = \mathcal{C}(\rho(D_i)b_i) \in \mathbb{F}^X$. Pick $r \in X$ at random from the support of y.
2. For $j = 1, \ldots, q$ query w at location: $(g_j h_i)^{-1} \cdot r \in X$.
3. Calculate $n_i = \sum_{j=1}^{q} c_j w[(g_j h_i)^{-1} \cdot r]$.
4. Return $m_i = y[r]^{-1} n_i$.

In order to show that this algorithm is a c-smooth decoder we need to show that:

- Completeness, i.e., if $w = \mathcal{C}(\sum m_i b_i)$ then the algorithm returns m_i on input i.
- Smoothness, i.e., each query is uniformly distributed over a domain of size $c|X|$.

[4]Note that this is the only place where we use the irreducibility of (ρ, V). We discuss it later in Section 6.

Completeness: Recall that by definition of the permutational representation it holds that $\tau(g)w[r] = w[g^{-1}r]$. Thus n_i (line 3 of the decoding algorithm) is equal to

$$n_i = \sum_{j=1}^{q} c_j w[(g_j h_i)^{-1} \cdot r] = (\tau(D_i)w)[r] \ .$$

Let us substitute $w = \mathcal{C}(\sum_j m_j b_j)$ in this equation.

$$n_i = (\tau(D_i)w)[r] = (\tau(D_i)\mathcal{C}(\sum_{j=1}^{k} m_j b_j))[r] \stackrel{1}{=} \mathcal{C}\left(\rho(D_i)\sum_{j=1}^{k} m_j b_j\right)[r] \tag{3.1}$$

$$= \sum_{j=1}^{k} m_j \mathcal{C}(\rho(D_i)b_j)[r] \stackrel{2}{=} m_i \mathcal{C}(\rho(D_i)b_i)[r] \ .$$

Here Equality 1 holds since $\mathcal{C}$ is a homomorphism of the representations ρ and τ and Equality 2 follows from Lemma 3.2. Thus from the definition of y it follows that $n_i = m_i y[r]$. Therefore, the algorithm returns a correct answer at line 4.

Smoothness: Note that if r is uniformly distributed over a domain of size $c|X|$, then so is $g_j h_i \cdot r$. Thus we need to prove that r is uniformly distributed over a domain of size $c|X|$, This is equivalent to say that the support of y is of size $c|X|$.

Since $\rho(D)$ is of rank one it holds that $\mathrm{Im}\,\mathcal{C} \cdot \rho(D)$ is one dimensional. Therefore, from Condition 2 if follows that for every non-zero vector in $\mathrm{Im}\,\mathcal{C} \cdot \rho(D)$ has support of size at least $c|X|$. Note that $y = \mathcal{C}(\rho(D * h_i)b_i) = \mathcal{C} \cdot \rho(D)(\rho(h_i)b_i)$. Thus $y \in \mathrm{Im}\,\mathcal{C} \cdot \rho(D)$ and from Lemma 3.2 it follows that $y \neq 0$.

□

3.1 Example: Two Query LDC from Representations of S_n

The goal of this subsection is to give a concrete example of irreducible representation which allows to construct two query LDC from Theorem 3.1. We want to mention that Hadamard Code can be captured by generalization of Theorem 3.1 see Section 6.2 for more details. The example given in this section has slightly worse parameters, but it is much simpler.

Let $\mathbb{F}$ be any algebraically closed field. The group S_n has a natural action on $[n]$. This action defines representation ρ on $\mathbb{F}^n$. This representation decomposes into a trivial representation which is spanned by vector of all ones and its complement which is the set of all vectors with sum zero. Let V be this representation, i.e., $V = \{v \in \mathbb{F}^n | \sum_{i=1}^{n} v[i] = 0\}$. One can show that this is indeed an irreducible representation. We denote it by ρ_1. Consider $f = id - (1,2) \in \mathbb{F}[S_n]$ then we claim that rank of $\rho_1(f)$ is one. Indeed let $\vec{x} = (x_1, x_2, \ldots, x_n) \in V$ then $\rho_1(f)(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n) - (x_2, x_1, x_3, \ldots, x_n) = (x_1 - x_2, x_2 - x_1, 0, \ldots, 0) \in V$. Thus $\mathrm{Im}\,\rho_1(f)$ is $\lambda(1, -1, 0, 0, \ldots, 0)$. Therefore $\mathrm{Rank}(\rho_1(f)) = 1$. Theorem 1.1 gives us immediately a 2 query $[n-1, n!]$ LDC.

Now let us show that using different sets X on which group S_n acts we can achieve tradeoff rate/soundness. Now let X be the set of all subsets of $[n]$ of size k. Then there exist a natural action of S_n on X which gives us permutational representation $\mathbb{F}^X$ (we think of $\mathbb{F}^X$ as all functions from subsets of size k to $\mathbb{F}$). Let us define $\mathcal{C}(x_1, x_2, \ldots, x_n) = g$ where g is a function which takes subset of size k as input and outputs the sum of this subset, i.e., g defined by

$$g(S) = \sum_{j \in S}^{k} x_j.$$

We can see that the support of $\mathcal{C}(\rho_1(f)) = \mathcal{C}(1, -1, 0, \ldots, 0)$ is all subsets which contains exactly one of the elements: 1 or 2. Thus it has relative support of size $2\frac{k}{n}\frac{n-k}{n}$. Using Theorem 3.1 we get two-query locally decodable codes $[n-1, \binom{n}{k}]$ with soundness $2\frac{k}{n}\frac{n-k}{n}$. This example shows that the parameters of the LDC depends not only on the representation it defines but also on the space in which we embed it into.

3.2 Embedding to the Regular Representation

Theorem 3.1 shows that in order to construct an LDC it is sufficient to do two things: First, construct an irreducible representation with a sparse rank one element. Second, embed it into a permutational representation such that the second condition of the theorem is satisfied. In this subsection we show that we can always embed any representation into the regular representation in a way that satisfies the second condition of the theorem.

Lemma 3.3. *Let V be a vector space over a field $\mathbb{F}$. Then for every irreducible representation (ρ, V) and for every $v \in V,\ v \neq 0$ there exist a homomorphism $\mathcal{C} : V \to \mathbb{F}[G]$ of representations (ρ, V) and the regular representation in $\mathbb{F}[G]$ such that supp$(\mathcal{C}(v)) \geq |G|(1 - \frac{1}{|\mathbb{F}|})$.*

Proof. We view $\mathbb{F}[G]$ as a left representation of G. That is, $\tau(g)(f) = g * f$. For any $u \in V^*$ let us define a mapping $T_u : V \to \mathbb{F}[G]$ by:

$$T_u(x) = \sum_{g \in G} (\bar{\rho}(g)u(x))g. \tag{3.2}$$

We claim that T_u is an homomorphism from the representation (ρ, V) to regular representation $\mathbb{F}[G]$. Indeed:

$$T_u(\rho(h)x) = \sum_{g \in G} \bar{\rho}(g)u(\rho(h)x)g = h * \sum_{g \in G} u(\rho(g^{-1}h)x)h^{-1}g.$$

Substituting $g = h^{-1}g$ we get

$$T_u(\rho(h)x) = h * \sum_{g \in G} u(\rho(g^{-1})x)g = \tau(h)T_u(x).$$

Now we want to show that for some $u \in V^*$ vector $T_u(v)$ has large support. Consider the set $U = \{T_u(v) : u \in V^*\}$. It is easy to see that it is a linear subspace of $\mathbb{F}[G]$ and that it have full support. From Lemma 2.5 it follows that there exists a vector with support at least $|G|(1 - \frac{1}{|\mathbb{F}|})$. Therefore, exist an u such that T_u is a G-homomorphism such that $T_u(v)$ has desired support. □

Note that when $\mathbb{F}$ is infinite field then we can get full support and all algebraically closed fields are infinite. As a corollary the last lemma we get Theorem 1.1.

Corollary 3.4 (Theorem 1.1)**.** *Let V be a vector space over an algebraically closed field $\mathbb{F}$. Let G be a finite group and let (ρ, V) be an irreducible representation of G. Let $D \in \mathbb{F}[G]$ be an element of group algebra of sparsity q such that $\mathrm{Rank}(\rho(D)) = 1$. Then there exist locally $(q, \delta, q\delta)$ decodable code $\mathcal{C} : V \to \mathbb{F}^G$.*

Assume that we have $(\rho, V), D \in \mathbb{F}[G]$ which satisfies the first condition of Theorem 3.1. Then from the corollary above it follows that we can embed (ρ, V) to the regular representation in a way that satisfies the second condition. A natural question to ask is can we embed it to a smaller permutational representation. The next lemma gives characterization of all such permutational representations.

Lemma 3.5. *Let $(\rho, V), D \in \mathbb{F}[G]$ which satisfies the first condition of Theorem 3.1. Let $v \in \mathrm{Im}\,\rho(D)$ a non-zero vector and $H < G$ is any subgroup of G. Assume that exist $u \in V^*$ such that $\rho(h)u = u$ for every $h \in H$ and $|\{g \in G/H : u(\rho(g)v) \neq 0\}| \geq c|G/H|$ then there exist G-homomorphism $C : V \to \mathbb{F}^X$, where $X = G/H$, such that supp$(C(v)) \geq c|X|$, i.e., it satisfies the second condition of Theorem 3.1.*

Proof. Consider a subspace L_H of the regular representation $\mathbb{F}^G$ of functions constant on cosets of H, i.e., $L_H = \{f \in \mathbb{F}^G : \forall g \in G, \forall h \in H, f(gh) = f(g)\}$. It is easy to see that L_H is a sub-representation of the regular representation isomorphic to the permutational representation $\mathbb{F}^X$, where $X = G/H$. Let T_u be an embedding as in proof of Lemma 3.3 defined by Equation 3.2. Note that since $Hu = u$ for every $x \in V, h \in H_u$ it holds that $T_u(x)[g] = T_u(x)[gh]$, i.e., $T_u(x) \in L_H$. Therefore T_u is an embedding to the permutational representation $\mathbb{F}^X$, where $X = G/H_u$. From the definition of T_u it follows that the support of $T_u(v)$ is exactly $|\{g \in G/H_u : u(\rho(g)v) \neq 0\}|$. □

Remark 3.6. It could be shown that any embedding satisfying second condition of Theorem 3.1 could be decribed by Lemma 3.5.

3.3 Alphabet Reduction

In this section we show that we can transform codes over any algebraic extension of $\mathbb{F}_p$ to codes over $\mathbb{F}_p$. The reduction which we give here adapts the reduction from [Efr09] to our settings.

Theorem 3.7. *Let $\mathbb{F}$ be a field of characteristic p and let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^X$ be a $(q, \delta, \frac{q\delta}{c})$-LDC as in Theorem 3.1. Then there exist a code $\tilde{\mathcal{C}} : \mathbb{F}_p \to \mathbb{F}_p^{X \times [q]}$ which is $(q, \delta, \frac{p}{p-1}\frac{q\delta}{c})$-LDC.*

Proof. First let us rescale the basis so that we will have the same decoding vector for every message symbol. Let v be any vector in $\mathrm{Im}(\rho(D))$. Set $y = \mathcal{C}(v)$. Recall that in the proof of Theorem 3.1 we have showed that $\mathcal{C}(\rho(D_i)b_i) = \lambda_i y$. We can replace b_i with $\lambda_i^{-1} b_i$ so that $\mathcal{C}(\rho(D_i)b_i) = y$. It follows from the assumption that y has support $c|X|$. For a linear functional $\ell : \mathbb{F} \to \mathbb{F}_p$, we denote by $\ell(y)$ vector achieved by applying ℓ on each coordinate of y. From standard random argument

there exists a linear functional ℓ such that support of $\ell(y)$ is at least $\frac{p-1}{p}c|X|$. Let us fix such an ℓ. Let $D = \sum_{i=1}^{q} c_i g_i \in \mathbb{F}[G]$ be a rank one element. Let us define $\tilde{\mathcal{C}}$ by $\tilde{\mathcal{C}}(m)[x,i] = \ell(c_i \mathcal{C}(m)[x])$. We need to show that this is an LDC. Let us describe the decoding algorithm:

Input: An oracle access to $w \in \mathbb{F}^X$ and bit index i.
Let $D_i = D * h_i = \sum_{j=1}^{q} c_j \cdot g_j h_i$ be where $h_i \in G$ is a group element as in Lemma 3.2.

1. Set $y = \mathcal{C}(\rho(D_i)b_i) \in \mathbb{F}^X$. Pick r at random from the support of $\ell(y)$.
2. For $j = 1, \ldots, q$ query w at location: $((g_j h_i)^{-1} \cdot r, j)$.
3. Calculate $\tilde{n}_i = \sum_{j=1}^{q} w[(g_j h_i)^{-1} \cdot r, j]$.
4. Return $m_i = \ell(y[r])^{-1} \tilde{n}_i$.

Now let us show that this decoding algorithm returns the correct answer when it receives an uncorrupted codeword. If $w = \tilde{\mathcal{C}}(m)$, then

$$\tilde{n}_i = \ell(\sum_{j=1}^{q} c_j \mathcal{C}((g_j h_i)^{-1} r)) = \ell(\tau(D_i)\mathcal{C}(m)[r]).$$

Recall that from Equation 3.1 it follows that $\tau(D_i)\mathcal{C}(m)[r] = m_i y[r]$. Thus we get that $\tilde{n}_i = m_i \ell(y[r])$. Thus, the decoding algorithm returns the correct answer on line 4 on an uncorrupted codeword.

Now let us prove that if $\tilde{\mathcal{C}}(m)$ is corrupted in at most δ coordinates, then the decoder reads a corrupted place with probability at most $\frac{p}{p-1}\frac{q\delta}{c}$. Let us call the coordinates of type (x,i) the i^{th} block. Let δ_i proportion of coordinates i^{th} block which are corrupted, and notice that $\sum \delta_i = q\delta$. Note that i^{th} query is distributed uniformly over $\frac{p-1}{p}c$ fraction of coordinates of the i^{th} block. Therefore, the probability that i^{th} coordinate is corrupted is $\frac{p}{p-1}\frac{\delta_i}{c}$. Thus by union bound we get that at least one of the coordinates is corrupted with probability at most $\sum \frac{p}{p-1}\frac{\delta_i}{c} = \frac{p}{p-1}\frac{q\delta}{c}$. □

We have the following corollary from this theorem and Theorem 1.1.

Corollary 3.8. *Let $\mathbb{F}$ be a field of characteristic p. Let G be a finite group and let (ρ, V) be an irreducible representation of G and let $k = \dim V$. Let $D \in \mathbb{F}[G]$ be an element of group algebra of sparsity q such that $\mathrm{Rank}(\rho(D)) = 1$. Then there exist $(q, \delta, \frac{p}{p-1}q\delta)$-LDC $\mathcal{C} : \mathbb{F}_p^k \to \mathbb{F}_p^{G\times[q]}$.*

4 Matching Vector Codes and Abelian Invariant Codes

In the next two sections we show that there exists irreducible representations such that Theorem 3.1 gives codes matching the parameters of [Efr09]. We show that the codes constructed in [Efr09] could be interpreted as a construction of an irreducible representation.

In this section we show that if MV is an orbit of a group H then one can construct from such MV an irreducible representation with a sparse element in the group algebra of rank one. In the next

section, we show that the variant of the Grolmusz's [Gro00] construction described in [Efr09],[5] is MV that is an orbit of the symmetric group.

Let A be an Abelian group. Recall that *the dual group* A^* is the set of all group homomorphisms $v : A \to \mathbb{Z}_m$, where m is the order of the group. In this paper it will be more convenient for us to work with the following generalization of MV to any Abelian group:

Definition 4.1. *Let A be an Abelian group. Let m be the order of A. For any set $S \subset \mathbb{Z}_m$ the families $\mathcal{U} = \{u_i\}_{i=1}^k \subset A, \mathcal{V} = \{v_i\}_{i=1}^k \subset A^*$ are* S-Matching Vectors(MV) *if the following conditions hold:*

1. *$v_j(u_i) \in S$ for every $i \neq j$.*
2. *$v_i(u_i) \notin S$ for every $i \in [k]$.*

Note that if $A = \mathbb{Z}_m^h$ using the isomorphism $\psi : A \to A^*$ given by $\psi(v)(x) = \langle v, x \rangle$ we get the standard definition of MV.

In this section we assume that the characteristics of $\mathbb{F}$ is co-prime to m and that there exists $\gamma \in \mathbb{F}^*$ an element of order m, i.e., $\gamma^m = 1$ and $\gamma^i \neq 1$ for $0 < i < m$. Then for any $v \in A^*$ we denote by γ^v the function from A to $\mathbb{F}$ defined by $\gamma^v(a) = \gamma^{v(a)}$. Let H be any *group that acts on the group* A. (Recall Definition 2.5 of an action of a group on a group.) In this case H also acts on A^*, where an action is given by the rule: $(h \cdot v)(x) = v(h^{-1} \cdot x)$. The group $G = A \rtimes H$ by Definition 2.6 acts on the set A. Let $(\tau, \mathbb{F}^A)$ be the corresponding permutational representation of G.

Definition 4.2. *A polynomial $p(x) \in \mathbb{F}[x]$ is S-decoding if $p(\gamma^s) = 0$ for all $s \in S$ and $p(1) = 1$.*

The goal of this section is to prove the following theorem:

Theorem 4.1. *Let $\mathcal{U}, \mathcal{V}$ be S-Matching Vectors such that $\mathcal{V}$ is an orbit of H. Let $p(x)$ be an S-decoding polynomial of sparsity q. Then there exists an irreducible representation (ρ, L), a permutational representation $(\tau, \mathbb{F}^A)$ of $G = A \rtimes H$ and $D = \sum_{i=1}^q c_i g_i$ which satisfy the conditions of Theorem 3.1 with $c = 1, \dim L = |\mathcal{V}|$.*

Proof. First we need to construct a representations (L, ρ). We do it in next two lemmas.

Lemma 4.2. *For any $\mathcal{V} \subset A^*$, the vector space $L \subset \mathbb{F}^A$ defined by*

$$L = \mathrm{Span}\{\gamma^v : v \in \mathcal{V}\} \subset \mathbb{F}^A \tag{4.1}$$

is a sub-representation of the regular representation of group A of dimension $|\mathcal{V}|$.

Proof. First let us show that L is closed under action of A. For any $v \in A^*$ it holds that:

$$\gamma^v(a + b) = \gamma^{v(a+b)} = \gamma^{v(a)+v(b)} = \gamma^{v(a)}\gamma^{v(b)} = \gamma^v(a)\gamma^v(b).$$

Thus γ^v is a one-dimensional sub-representation of the regular representation of the group A. Therefore, L is a sub-representation. Note that for $v_1 \neq v_2$, the representations $\gamma^{v_1}, \gamma^{v_2}$ are non isomorphic one-dimensional sub-representations. Therefore, from Lemma 2.4 it follows that $\{\gamma^v\}_{v \in \mathcal{V}}$ are linearly independent vectors. Thus the dimension of L is $|\mathcal{V}|$. □

[5] Using the same ideas it is also possible to prove the statement for Grolmusz's construction.

Lemma 4.3. *For any $\mathcal{V} \subset A^*$ closed under action of H it holds that the vector space L defined by Equation 4.1 is a sub-representation of the permutational representation $(\tau, \mathbb{F}^A)$ of the group $G = A \rtimes H$.*

Proof. Let $v \in A^*$ and consider the vector $\gamma^v \in \mathbb{F}^A$. Then for $h \in H$ it holds that

$$(\tau(h)\gamma^v)(x) = \gamma^{v(h^{-1}x)} = \gamma^{h\cdot v}(x) \ .$$

Thus if $\mathcal{V}$ is closed under the action of H then the vector space L is closed under the action of $\tau(h)$ for $h \in H$. Since L is a representation of A, it is also closed under the action of $\tau(a)$ for $a \in A$. Since H and A generate G, the space L is a sub-representation of $(\tau, \mathbb{F}^A)$. □

Let us denote this sub-representation by (ρ, L) and by $\mathcal{C} : L \to \mathbb{F}^A$ its embedding into $\mathbb{F}^A$. Note that $\dim L = |\mathcal{V}|$.

Lemma 4.4. *If H acts transitively on $\mathcal{V}$ then the representation (ρ, L) of G is irreducible.*

Proof. Assume that $\tilde{L} \subset L$ is a non-zero sub-representation of L. In order to prove that (ρ, L) is an irreducible representation we need to prove that $\tilde{L} = L$. Since $\tilde{L}$ is a representation of A for some $v \in \mathcal{V}$ it holds that $\gamma^v \in \tilde{L}$. Since H acts transitively on $\mathcal{V}$ for every $v' \in \mathcal{V}$ there exists $h \in H$ such that $h \cdot v = v'$. Thus it holds that

$$\tau(h)\gamma^v = \gamma^{h\cdot v} = \gamma^{v'} \ .$$

Therefore, we proved that:

$$L = \mathrm{Span}\{\gamma^v : v \in \mathcal{V}\} \subset \tilde{L} \subset L.$$

Thus $\tilde{L} = L$. □

Let $p(x) = \sum_{i=1}^{q} c_i x^{t_i}$ be the given S-decoding polynomial. We define D as $D = \sum_{i=1}^{q} c_i(t_i u_1)$, where we think of $t_i u_1$ as an element of G. We claim that $\mathrm{Rank}\, \rho(D) = 1$.

Note that the set $\{\gamma^{v_i}\}_{i=1}^{k}$ forms a basis of L. Let us show that $\rho(D)\gamma^{v_i} = 0$ for $i \neq 1$ and $\rho(D)\gamma^{v_1} = \gamma^{v_1}$. Indeed:

$$\rho(D)\gamma^{v_i} = \sum c_i \rho(t_i u_1)\gamma^{v_i} = \gamma^{v_i} \sum c_i \gamma^{v_i(t_i u_1)} = \gamma^{v_i} \sum c_i (\gamma^{v_i(u_1)})^{t_i} = \gamma^{v_i} p(\gamma^{v_i(u_1)}).$$

Note that for natural embedding of $\mathcal{C} : L \to \mathbb{F}^A$ it holds that $\mathrm{Im}\, \mathcal{C}(\rho(D)) = \mathrm{Span}\{\gamma^{v_1}\}$ has full support. Therefore, smoothness constant c in Theorem 3.1 is 1. □

Remark 4.5. The representation of (ρ, L) defined in the proof is: $\mathrm{Ind}_{A\rtimes F}^{G} \gamma^v$, where v is any element in $\mathcal{V}$ and $F = \{h \in H : h \cdot v = v\}$ be a subgroup of H.

Note that in the proof of the above theorem we used only one element u_1 of $\mathcal{U}$. The following lemma shows that if $\mathcal{V}$ is an orbit of some group and "matching" one element then we can construct $\mathcal{U}$ to be orbit of the same group such that $\mathcal{U}, \mathcal{V}$ are Matching Vectors.

Lemma 4.6. *Let $\mathcal{V} = \{h_i \cdot v\}_{i=1}^{k} \subset A^*$ be an orbit of H such that for some $u \in A$ it holds that $h_1 v(u) = 0$ and $h_i v(u) \in S$ for $i \neq 1$. Then the family $\mathcal{U} = \{h_i u\}_{i=1}^{k}, \mathcal{V} = \{h_i \cdot v\}_{i=1}^{k}$ is a family of S-Matching Vectors.*

Proof. First note that $h_i v(h_i u) = h_i^{-1} h_i v(u) = v(u) = 0$. Next for $i \neq j$ it holds that $h_i v(h_j u) = h_j^{-1} h_i v(u)$. Since $\mathcal{V}$ is an orbit there exist k such that $h_j^{-1} h_i v = h_k v$, $k \neq 1$ since $i \neq j$. Therefore $h_i v(h_j u) = h_k(u) \in S$. □

5 Symmetry and Matching Vectors

The goal of this section is to show that the variant of the Grolmusz's [Gro00] construction described in [Efr09] is *symmetric* MV that is an orbit of the symmetric group (let us call it H). The construction from [Efr09] starts from the base construction with $S = \mathbb{Z}_m - \{0\}$ and next it reduces the size of S using the tensor power. In order to show that this construction is an orbit of H, we observe that the base construction is an orbit of H. Next we define an action of H on the tensor power of group such that the tensor power of orbit of H remains an orbit of H. For the sake of completeness, we review here the variant of the Grolmusz's [Gro00] construction.

Let us define a tensor product and action of group on it.

Tensor Product

Definition 5.1 (Tensor Product of Abelian Groups)**.** *Let A, B be Abelian groups. Then tensor product of A and B, denoted by $A \otimes B$, is an Abelian group generated by $\{a \otimes b : a \in A, b \in B\}$ with relations*

$$\begin{aligned}(a_1 + a_2) \otimes b_1 &= a_1 \otimes b_1 + a_2 \otimes b_1 \\ a_1 \otimes (b_1 + b_2) &= a_1 \otimes b_1 + a_1 \otimes b_2\end{aligned}$$

for every a_1, a_2, b_1, b_2.

For example, if $A = \mathbb{Z}_m^h$, then $A \otimes A = \mathbb{Z}_m^{h^2}$. There exist a canonical isomorphism between $A^* \otimes B^*$ and $(A \otimes B)^*$. For $v_1 \in A^*, v_2 \in B^*$ we define a mapping on the generators by: $v_1 \otimes v_2(u_1 \otimes u_2) = v_1(u_1)v_2(u_2)$ for every u_1, u_2 and extend it by linearity.

If some group H acts on the groups A and B, then we can define an action of H on generators of $A \otimes B$ by the rule $h \cdot (a \otimes b) = (h \cdot a) \otimes (h \cdot b)$ and extend it by linearity. The tensor power $A^{\otimes k}$ is just tensor product of A with itself k times. Consider the mapping $P^k : A \to A^{\otimes k}$ defined by:

$$P^k(u) = \underbrace{u \otimes u \otimes \ldots \otimes u}_{k \text{ times}} .$$

From the definition of action on tensor product it follows that

$$P^k(h \cdot u) = h \cdot P^k(u) . \tag{5.1}$$

Thus if $\mathcal{U}$ is an orbit of H then $P^k(\mathcal{U})$ is also an orbit of H. For $v \in A^*, u \in A$ it holds that

$$P^k(v)(P^k(u)) = v(u)^k . \tag{5.2}$$

Theorem 5.1. *For every integer $k > 0$ there exists an integer $m = p_1 p_2$ and a set $S = \{p_1, p_2, p_1 + p_2\} \subset \mathbb{Z}_m$ and families $\mathcal{U} \subset A, \mathcal{V} \subset A^*$ of S-Matching Vectors, where $\mathcal{U}, \mathcal{V}$ are orbits of the symmetric group, such that $|\mathcal{V}| \geq k$ and $|A| \leq \exp\exp(O(\sqrt{logk \log\log k}))$.*

Proof. We start from the base construction of MV and show that this construction is an orbit of a symmetric group. Next we make transformations on this construction and we show that such transformation maps orbit to orbit.

Base Construction In the base construction $B = \mathbb{Z}_m^h$ and each subset of size $m-1$ of $[h]$ we set u_i to be its indicator. Set $v_i(x) = \langle x, u_i \rangle$. It is easy to see $v_i(u_i) = m-1$ and $v_i(u_j) \neq m-1$ for $j \neq i$. Let $H = S_h$ act on $\mathbb{Z}_m^h$ by permuting its coordinates. Then it is easy to see that $\mathcal{U}$ and $\mathcal{V}$ are orbits of S_h. For sake of simplicity let us add one additional coordinate to B so that $B = \mathbb{Z}_m^{h+1}$ and set all u_i, v_i to be one on this coordinate. Now we have that $v_i(u_i) = 0$ and $v_i(u_j) \neq 0$. Thus $\mathcal{U} = \{u_i\}, \mathcal{V} = \{v_i\}$ are S-MV, where $S = \mathbb{Z}_m - \{0\}$.

Reducing size of S: Let us assume that $m = p_1 p_2$ where p_1, p_2 are primes. Now assume that $\mathcal{U}, \mathcal{V}$ be any S-MV with $S = \mathbb{Z}_m - \{0\}$. Let us show how to reduce size of S to 3. Let us set the Abelian group $A = B^{\otimes p_1 - 1} \oplus B^{\otimes p_2 - 1}$. Consider a mapping $R : B \to A$ defined by:

$$R(u) = \left(p_2 P^{p_1-1}(u), p_1 P^{p_2-1}(u)\right) .$$

In the same way let us define R on dual group by:

$$R^*(v) = \left(P^{p_1-1}(v), P^{p_2-1}(v)\right) .$$

Let us define action of H on the direct sum coordinate-wise i.e., $h \cdot (a, b) = (h \cdot a, h \cdot b)$. From Equation 5.1 it follows that $h \cdot R^*(v) = R^*(h \cdot v)$. Thus it holds that if $\mathcal{V}$ is the orbit of group H then $R^*(\mathcal{V})$ is also the orbit of H. Therefore we proved that:

Lemma 5.2. *The mapping R, R^* maps orbits to orbits.*

From this lemma it follows that if we apply R, R^* on the base construction we get orbit of the symmetric group. The rest of the proof shows that for suitable choice of parameters this will give us parameters as in the theorem.

First let us show that $S = \{p_1, p_2, p_1 + p_2\}$. From the Equation 5.2 it follows that for any $u \in B, v \in B^*$ it holds that:

$$R^*(v)(R(u)) = p_2 v(u)^{p-1} + p_1 v(u)^{p_2-1} = f(v(u)) ,$$

where $f(x) = p_2 x^{p_1-1} + p_1 x^{p_2-1}$.

Claim 5.3. *$f(x) \in \{p_1, p_2, p_1 + p_2\}$ for $x \neq 0$ and $f(0) = 0$.*

Proof. For $x = 0$ the claim is trivial. Let $x \neq 0$. Then $f(x) \mod p_1 = p_2 x^{p_1-1}$. If $x = 0 \mod p_1$ then $f(x) = 0 \mod p_1$. From Fermat little theorem it follows that $f(x) = p_2 \mod p_1$ if $x \neq 0 \mod p_1$. Thus $f(x) \in \{0, p_2\} \mod p_1$. The same holds modulo p_2. Thus from Chines Reminder Theorem it follows that $f(x) \in \{0, p_1, p_2, p_1 + p_2\}$. Note that $f(x) = 0$ implies that $x = 0$. □

Therefore, $R(\mathcal{U}), R^*(\mathcal{V})$ (where $\mathcal{U}, \mathcal{V}$ is the base construction) are S-Matching Vectors with $S = \{p_1, p_2, p_1 + p_2\}$.

Setting Parameters Let us take $p_1 \approx p_2 = O(\sqrt{m})$ and $h = m^2$. Then $|\mathcal{V}| = \binom{h}{m-1} = \exp(O(m \log m))$ and $|A| = m^{h^{p_1-1}} + m^{h^{p_2-1}} = \exp\exp(\sqrt{m}\log m)$. Note that $\log|\mathcal{V}| = O(m \log m)$. Therefore

$$|A| = \exp\exp(O(\sqrt{\log|\mathcal{V}| \log\log|\mathcal{V}|}))$$

□

6 Is Irreducibility Essential?

Representation theory when characteristic of the field divides the size of the group called modular representation theory. Modular representation theory is very different from non-modular case. In this section we ask the question does irreducibility in Theorem 3.1 essential. We show that in non-modular case the answer is Yes[6]. We show that in modular case we can construct reducible representation which will lead to LDC. Thus we can see Theorem 6.1 as a generalization of the Theorem 3.1 to modular representation theory.

It may happen that some representation is irreducible over field $\mathbb{F}$, but reducible over algebraic closure of $\mathbb{F}$. Representations which are irreducible over algebraic closure of $\mathbb{F}$ called completely irreducible. Although for the proof of the Theorem 3.1 we do not need complete irreducibility we show that in order to have rank one element complete irreducibility is essential for non-modular representations.

In the proof of Theorem 3.1, the only reason why we need the fact that (ρ, V) is irreducible is to show that the orbit of u spans all the dual space. Therefore, we can make the following generalization of Theorem 3.1:

Theorem 6.1. *Let G be a finite group. Let (ρ, V) be any representation of G ,$(\tau, \mathbb{F}^X)$ be a permutational representation of G. Let $\mathcal{C} : V \to \mathbb{F}^X$ be a G-embedding. Assume that the following conditions hold:*

1. *(a) There exists a q-sparse element $D \in \mathbb{F}[G]$, $D = \sum_{i=1}^{q} c_i g_i$ such that $\mathrm{Rank}(\rho(D)) = 1$.*
   (b) Let $u \in V^*$ be a non-zero linear functional such that $\mathrm{Ker}\, u = \mathrm{Ker}\, \rho(D)$. Then the set $\{\bar{\rho}(g)u | g \in G\}$ spans V^*.
2. *$\mathrm{Im}(\mathcal{C} \circ \rho(D))$ has a support $c|X|$.*

Then there exists a basis $b_1, \ldots, b_k$ for V such that $\mathcal{C}(\sum(m_i b_i))$ is$(q, \delta, \frac{q\delta}{c})$-LDC.

From Lemma 2.3 it follows that irreducibility of the representation (ρ, V) implies Condition 1b of this theorem. Here we show that if characteristics of the field $\mathbb{F}$ is does not divides $|G|$ then the converse is also true, i.e., if u spans dual space V^* then (ρ, V) is irreducible.

[6]In fact we show that the representation should be indecomposable. In non-modular case all indecomposable representations are irreducible.

6.1 Yes!

Theorem 6.2. *Let V be a vector space over an algebraically closed field $\mathbb{F}$ of characteristic which does not divides $|G|$. Let ρ be a representation of group G in the vector space V. Let $f \in \mathbb{F}[G]$ such that $\operatorname{Rank}\rho(f) = 1$. Let $u \in V^*$ such that $\operatorname{Ker} u = \operatorname{Ker}\rho(f)$. If $V^* = \operatorname{Span}\{\bar{\rho}(g)u | g \in G\}$, then V is an irreducible representation.*

Proof. Let us assume by contradiction that V is reducible. Then from Theorem 2.2 it follows that $V = V_1 \oplus V_2$. This mean that in basis of V_1 and V_2 for every $g \in G$ the matrix $\rho(g)$ is of form

$$\rho(g) = \begin{pmatrix} \rho_1(g) & 0 \\ 0 & \rho_2(g) \end{pmatrix} ,$$

where ρ_1, ρ_2 restrictions of ρ to V_1, V_2. Therefore $\rho(f) = \sum a_i \rho(g_i)$ is of form

$$\rho(f) = \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} .$$

But this matrix may be of rank one only if A or B is zero. Let us assume w.l.g. that B is zero. But then $V_2 \subset \operatorname{Ker}\rho(f)$. Therefore it holds that $u(V_2) = 0$. Since V_2 is invariant space, it also holds that $\bar{\rho}(g)u(V_2) = 0$. Since $\bar{\rho}(g)u$ span V^*, it must be that $V_2 = 0$. □

If V is a vector space over some field $\mathbb{F}$, then $\operatorname{Rank}\rho(f) = 1$ also over algebraic closure of $\mathbb{F}$ and thus (ρ, V) should be irreducible not just over $\mathbb{F}$, but also over the algebraic closure of $\mathbb{F}$.

6.2 No!

Let us now give an example of reducible representations (ρ, V) when vector u spans all the dual space. Of course in this example characteristics of $\mathbb{F}$ divides $|G|$. This example is a well know Reed-Muller Code. Let $\mathbb{F}$ be a field of characteristic $p \geq d$. Let us consider the group G of affine transformations over $\mathbb{F}_p^k$, i.e., $G = \{A\vec{x} + b : A \in \mathrm{GL}(p,k), b \in \mathbb{F}_p^k\}$. Let us set $X = \mathbb{F}_p^k$ and $(\tau, \mathbb{F}^X)$ be corresponding permutational representation of G. Let $\mathrm{RM}(d,k) \subset \mathbb{F}^X$ be a vector space of polynomials of total degree at most d with coefficients in $\mathbb{F}$. It is easy to verify that $\mathrm{RM}(d,k)$ is invariant under permutations of G. Thus $\mathrm{RM}(d,k)$ is a sub-representation of $\mathbb{F}^X$. Let us denote it by $(\rho, \mathrm{RM}(d,k))$. Let $\mathrm{const} \subset \mathrm{RM}(d,k)$ be a subspace of constant functions. Note that const is a sub-representation of V. Thus $\mathrm{RM}(d,k)$ is reducible. Let us pick $\lambda \neq 1 \in \mathbb{F}_p$ be a generator of the $\mathbb{F}_p^*$. Let $m_\lambda \in G$ be a permutation $\vec{x} \mapsto \lambda\vec{x}$.

Lemma 6.3. *There exists $c_0, c_2, \ldots, c_d$ such that the following holds: Let $D = \sum c_i m_\lambda^i \in \mathbb{F}[G]$ then the mapping $\rho(D)$ is of rank one and given a polynomial $p \in \mathbb{F}^X$ the mapping $\rho(D)$ returns a constant function $p(\vec{0})$.*

Proof. Let us consider how $\rho(m_\lambda)$ acts on p. Let $p = \sum_{j=0}^{d} p_j$, where p_j is a homogeneous part of p of degree j. Then it holds that

$$\rho(m_\lambda)p(x) = p(\lambda^{-1}x) = \sum_{j=0}^{d} \lambda^{-j} p_j(x) .$$

In the same way it for every i it also holds that

$$\rho(m_\lambda^i)p(x) = p(\lambda^{-i}x) = \sum_{j=0}^{d} \lambda^{-ij} p_j(x) \ . \tag{6.1}$$

Let $V[i,j] = \lambda^{-ij}$ be a Vandermonde matrix. For vector $\vec{c} = (c_0, c_2, \ldots, c_d)$ let $a = (a_0, \ldots a_d) = V \cdot \vec{c}$. Then from Equation 6.1 it follows that:

$$\rho(\sum_{i=0}^{d} c_i m_\lambda^i)p = \sum_{i=0}^{d} a_i p_i \ . \tag{6.2}$$

Note that V is invertible matrix. Thus we can choose $\vec{c}$ such that $V \cdot \vec{c} = (1, 0, \ldots, 0)$. Substituting this $\vec{c}$ in Equation 6.2 we get:

$$\rho(\sum_{i=0}^{d} c_i m_\lambda^i) = p_0 \ .$$

But p_0 is a constant term of p which exactly equal to $p(\vec{0})$. □

Now consider a linear functional $u : \mathrm{RM}(d,k) \to \mathbb{F}$ given by $u(p) = p(\vec{0})$. Then definitely it holds that $\operatorname{Ker} u = \operatorname{Ker} \rho(D)$.

Lemma 6.4. *Then the set* $\{\bar{\rho}(g)u | g \in G\}$ *spans the dual space of* $\mathrm{RM}(d,k)$.

Proof. Note that linear functionals $u_1, u_2, \ldots, u_k$ span the dual space iff $\cap_{i=1}^{k} \operatorname{Ker} u_i = 0$. For $b \in \mathbb{F}_p^k$ let $g_b \in G$ be a permutation $x \mapsto x + b$. Let us show that:

$$\cap_{b \in \mathbb{F}_p^k} \operatorname{Ker} g_b u = 0 \ .$$

Indeed $g_b u(p) = p(b)$. Thus if $p \in \cap_{b \in \mathbb{F}_p^k} \operatorname{Ker} g_b u$ then $p(b) = 0$ for every $b \in \mathbb{F}_p^k$. Thus it must be that $p = 0$. □

Acknowledgements

I am grateful to Amnon Ta-Shma and Oded Regev for many helpful, in-depth discussions and for helpful comments on this paper. I want to thank to Dmitry Gourevitch, Venkatesan Guruswami, Alex Lubotzky, Zeev Rudnik , Avi Wigderson, and Chris Umans for very helpful conversions. I also want to thank to my wife Rivka for editing this paper for grammar mistakes.

References

[Efr09] Klim Efremenko. 3-query locally decodable codes of subexponential length. In *STOC*, pages 39–44, 2009.

[Gas04] William I. Gasarch. A survey on private information retrieval (column: Computational complexity). *Bulletin of the EATCS*, 82:72–107, 2004.

[GKST02] Oded Goldreich, Howard J. Karloff, Leonard J. Schulman, and Luca Trevisan. Lower bounds for linear locally decodable codes and private information retrieval. In *IEEE Conference on Computational Complexity*, pages 175–183, 2002.

[Gro00] Vince Grolmusz. Superpolynomial size set-systems with restricted intersections mod 6 and explicit ramsey graphs. *Combinatorica*, 20(1):71–86, 2000.

[IS08] Toshiya Itoh and Yasuhiro Suzuki. New constructions for query-efficient locally decodable codes of subexponential length. *CoRR*, abs/0810.4576, 2008.

[KdW03] Iordanis Kerenidis and Ronald de Wolf. Exponential lower bound for 2-query locally decodable codes via a quantum argument. In *STOC*, pages 106–115, 2003.

[KSY11] Swastik Kopparty, Shubhangi Saraf, and Sergey Yekhanin. High-rate codes with sublinear-time decoding. In *STOC*, pages 167–176, 2011.

[KT00] Jonathan Katz and Luca Trevisan. On the efficiency of local decoding procedures for error-correcting codes. In *STOC*, pages 80–86, 2000.

[MFL+10] Y. Meng Chee, T. Feng, S. Ling, H. Wang, and L. F. Zhang. Query-Efficient Locally Decodable Codes of Subexponential Length. *ArXiv e-prints*, August 2010.

[Ser77] Jean Pierre. Serre. *Linear representations of finite groups / Jean-Pierre Serre ; translated from the French by Leonard L. Scott*. Springer-Verlag, New York :, 1977.

[Tre04] Luca Trevisan. Some applications of coding theory in computational complexity. Technical Report 043, Electronic Colloquium on Computational Complexity (ECCC), 2004.

[Woo07] David Woodruff. New lower bounds for general locally decodable codes. *Electronic Colloquium on Computational Complexity (ECCC)*, 2007.

[Yek08] Sergey Yekhanin. Towards 3-query locally decodable codes of subexponential length. *J. ACM*, 55(1), 2008.

[Yek10] Sergey Yekhanin. Locally decodable codes. *Foundations and trends in theoretical computer science*, 2010.

A G-Invariant Codes and Representations of G

In this section we show tight connections between linear G-invariant codes and the representations of the group G. We show that there exists a one-to-one correspondence between subrepresentations of the permutational representations and G-invariant codes. Furthermore we can define a representation in the message space so that the code becomes a G-homomorphism.

Let us first define G-invariant codes:

Definition A.1. *Let G be a group acting on a set $X = \{x_i\}_{i=1}^n$. Let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^X$ be a code. We say $\mathcal{C}$ is G-invariant iff for every $c = (c_{x_1}, c_{x_2}, \ldots, c_{x_n}) \in \mathrm{Im}(\mathcal{C})$, and for every $g \in G$ it holds that*

$$g \cdot c = (c_{g^{-1} \cdot x_1}, c_{g^{-1} \cdot x_2}, \ldots, c_{g^{-1} \cdot x_n}) \in \mathrm{Im}(\mathcal{C}) \ .$$

The action of G on X defines a permutational representation $(\tau, \mathbb{F}^X)$ of G (see Equation 2.2). We claim that there is a one to one correspondence between linear G-invariant codes and sub-representations of $(\tau, \mathbb{F}^X)$.

Lemma A.1. *Let G be a group that acts on the set X. Let $(\tau, \mathbb{F}^X)$ be the permutational representation defined by this action. Let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^X$ be a linear code. Then $\mathcal{C}$ is G-invariant if and only if $\mathrm{Im}\,\mathcal{C}$ is a sub-representation of $(\tau, \mathbb{F}^X)$.*

Proof. The proof almost follows from the definition. Let $c \in \mathrm{Im}\,\mathcal{C}$, where $c = (c_{x_1}, c_{x_2}, \ldots, c_{x_n})$ and consider c as a function from X to $\mathbb{F}$. Then $(g \cdot c)(x) = c(g^{-1}x)$ and by the definition of τ we have that $(\tau(g)c)(x) = c(g^{-1}x)$. Thus the code $\mathcal{C}$ is G-invariant if and only if for every $c \in \mathrm{Im}(\mathcal{C})$ and for every $g \in G$ it holds that $\tau(g)c \in \mathcal{C}$ i.e., if and only if $\mathrm{Im}\,\mathcal{C}$ is a sub-representation of $(\tau, \mathbb{F}^X)$. □

As a corollary we get that G-homomorphisms into permutational representations are G-invariant codes.

Corollary A.2. *Let G be a group acting on X. Let $(\tau, \mathbb{F}^X)$ be the permutational representation defined by this action. Let $(\rho, \mathbb{F}^k)$ be any representation of G. Let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^X$ be a homomorphism of the representations $(\rho, \mathbb{F}^k)$ and $(\tau, \mathbb{F}^X)$ then $\mathcal{C}$ is a G-invariant code.*

Proof. This follows from Lemma A.1 and the fact that image of a G-homomorphism is a sub-representation. □

Let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^X$ be a linear one-to-one G-invariant code. We already know that $\mathrm{Im}(\mathcal{C})$ is a sub-representation of $(\tau, \mathbb{F}^X)$. Let us show that we can define a representation $(\rho, \mathbb{F}^k)$ such that $\mathcal{C}$ is a G-homomorphism.

Theorem A.3. *Let G be a group acting on X. Let $(\tau, \mathbb{F}^X)$ be the permutational representation defined by this action. Let $\mathcal{C} : \mathbb{F}^k \to \mathbb{F}^X$ be a linear one-to-one G-invariant code. Define a representation ρ of G in $\mathbb{F}^k$ by:*

$$\rho(g)(v) = \mathcal{C}^{-1}(\tau(g)\mathcal{C}(v)) \ . \tag{A.1}$$

Then $\mathcal{C}$ is an embedding of the representations $(\rho, \mathbb{F}^k)$ in $(\tau, \mathbb{F}^X)$.

Proof. First we need to proof that $\rho(g)$ is well defined: Since $\mathcal{C}$ is one-to-one $\mathcal{C}^{-1}$ is defined on $\mathrm{Im}\,\mathcal{C}$. Since $\mathcal{C}$ is closed under G it holds that $\tau(g)\mathcal{C}(v) \in \mathcal{C}$ therefore $\mathcal{C}^{-1}$ is defined on $(\tau(g)\mathcal{C}(v))$.

Now let us show that $\mathcal{C}$ is a G homomorphism:

$$\mathcal{C}(\rho(g)v) = \mathcal{C}(\mathcal{C}^{-1}(\tau(g)\mathcal{C}(v))) = \tau(g)\mathcal{C}(v) \ .$$

□

ECCC ISSN 1433-8092

http://eccc.hpi-web.de