Function-Correcting Codes

Andreas Lenz, *Student Member, IEEE*, Rawad Bitar, *Member, IEEE*,
Antonia Wachter-Zeh, *Senior Member, IEEE*, and Eitan Yaakobi, *Senior Member, IEEE*

***Abstract*— In this paper we study *function-correcting codes*, a new class of codes designed to protect the function evaluation of a message against errors. We show that FCCs are equivalent to *irregular-distance codes*, i.e., codes that obey some given distance requirement between each pair of codewords. Using these connections, we study irregular-distance codes and derive general upper and lower bounds on their optimal redundancy. Since these bounds heavily depend on the specific function, we provide simplified, suboptimal bounds that are easier to evaluate. We further employ our general results to specific functions of interest and compare our results to standard error-correcting codes, which protect the whole message.**

***Index Terms*— Forward error correction, error correction codes, information theory.**

I. Introduction

IN STANDARD communication systems, a sender desires to convey a message to a receiver via an erroneous channel. Classically, each part of the message is of equal importance to the receiver and the common goal is to construct an error-correcting code with a suitable decoder such that the whole message can be recovered correctly. Consider now the scenario where a certain *attribute* of the message, i.e., the result of evaluating a certain function on the message, is of particular interest to the receiver. Assuming that the sender is aware of this function, she can encode the message such that the desired attribute is protected against errors. This paradigm gives rise to a new class of codes, which we call *function-correcting codes* (FCCs). In this work we consider FCCs, where the message itself is observed through the channel, followed by redundancy, as illustrated in Fig. 1.

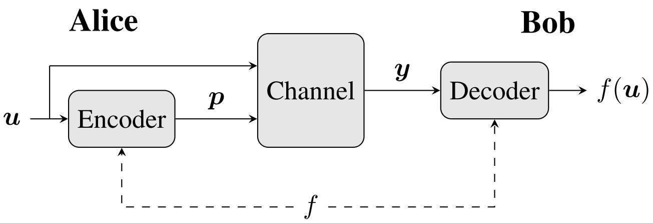


Fig. 1. Illustration of the FCC setup. Alice has a message $\boldsymbol{u}$, which features an attribute $f(\boldsymbol{u})$ that is of special interest to Bob. To guarantee recoverability of this attribute, Alice encodes the message $\boldsymbol{u}$ to a redundancy vector $\boldsymbol{p}$. Given an erroneous version $\boldsymbol{y}$ of the codeword $\boldsymbol{c} = (\boldsymbol{u}, \boldsymbol{p})$ and the knowledge of the function f, Bob can correctly infer $f(\boldsymbol{u})$.

Clearly, if the receiver is able to recover the message, it can evaluate the function on the message to obtain the desired attribute. It is however more efficient to protect only the specific function value of interest, especially when the message is long and the function image is small. Our generic goal when designing FCCs for a given function is to use the smallest amount of redundancy that allows the recovery of the attribute.

A key aspect for the design of FCCs is the topology of the function regions, i.e., the sets of message vectors that evaluate to the same function value. Since FCCs protect a specific function evaluation of the message, the receiver does not need to distinguish between codewords from messages that evaluate to the same function value. This means that the distance between any two codewords within one function region is irrelevant. On the other hand, codewords corresponding to different function values should have appropriate distances. Consequently, the redundancy vectors of an FCC have to fulfill an irregular distance profile, where each pair of redundancy vectors has to satisfy an individual distance constraint.

A. Application

The employment of FCCs can, for example, be beneficial in archival data storage. Consider a large data set, or message in our terminology, which is stored on a noisy storage medium. The message may be encoded with an error-correcting code to ensure reliability when retrieving it. Now assume that an attribute with highly sensitive information, which can be modeled as a function evaluation on the message is to be stored on the same medium. Due to the importance of this peculiar attribute, we desire to add an extra layer of protection for it. A natural solution is to encode the attribute with an error-correcting code with high error-correction capability. However, this idea is oblivious to the fact that the message is stored on the same storage medium. We propose to leverage this fact through the use of FCCs that may require less redundancy as we show in the sequel. When reading the message and its attribute through a noisy channel, errors may happen.

Manuscript received 13 July 2022; revised 11 January 2023; accepted 5 May 2023. Date of publication 24 May 2023; date of current version 18 August 2023. This work was supported in part by the European Research Council (ERC) under the European Union's Horizon 2020 Research and Innovation Program under Grant 801434, in part by the United States–Israel Binational Science Foundation (BSF) under Grant 2018048, and in part by the Technical University of Munich—Institute for Advanced Studies funded by the German Excellence Initiative and European Union Seventh Framework Program under Grant 291763. An earlier version of this paper was presented in part at ISIT 2021 [DOI: 10.1109/ISIT45174.2021.9517976]. *(Corresponding author: Andreas Lenz.)*

Andreas Lenz, Rawad Bitar, and Antonia Wachter-Zeh are with the Institute for Communications Engineering, Technical University of Munich (TUM), 80333 Munich, Germany (e-mail: andreas.lenz@mytum.de; rawad.bitar@tum.de; antonia.wachter-zeh@tum.de).

Eitan Yaakobi is with the CS Department, Technion—Israel Institute of Technology, Haifa 3200003, Israel (e-mail: yaakobi@cs.technion.ac.il).

Communicated by L. Dolecek, Associate Editor for Coding and Decoding.
Digital Object Identifier 10.1109/TIT.2023.3279768

To abstract the fact that more errors can happen in the message than the error-correcting code used to encode it can tolerate, we assume that a potentially noisy version of the data is available to the receiver. FCCs thus provide an individual level of protection to specific attributes of the message, offering higher flexibility and efficiency over classical error-correcting codes.

B. Related Works

Unequal error protection (UEP) codes [2], [3] allow a stronger protection of specific parts of the message. The connection between FCCs and codes for UEP manifests in the two levels of protection that FCCs provide to the message and the attribute. Since the message can either be unprotected or can itself be the codeword of an error-correcting code and the attribute is separately protected by the FCC, it is possible to control the error protection level of these parts. As the attribute is the evaluation of an arbitrary function on the message, it is also possible that it is simply a substring of the message, resulting in UEP for this part of the message. In general however, the attribute may be an arbitrary function of the message and hence, in this aspect, FCCs form a more general class of codes. On the other hand, UEP codes may protect an arbitrary number of attributes of interest.

In the context of random access memories, codes with unequal message protection have been designed in [4]. The authors construct codes that guarantee larger distances for codewords that stem from a specific predefined subset of messages. Similar to our work, the required distance varies between pairs of codewords. In contrast to our work, the distance requirement in [4] depends on groups to which the codewords are assigned, and here, as we will show later, we require an individual distance for each pair of codewords. For an information-theoretic study of both unequal error and message protection codes see [5].

Another related line of work [6], [7], [8] studies the scenario, where a sender wishes to communicate a message to a receiver such that the receiver can determine the evaluation of a function on their combined data. Therein, optimal transmission rates for which the recovery of the function evaluation is possible, are derived. There are several important aspects that differentiates our work from these papers. First, we study zero-error codes over an adversarial channel as opposed to non-zero, but vanishing error probabilities. Second, the message sent from Alice to Bob may contain errors in our setup. Notice however that [7] uses a characteristic graph [9], which is similar in spirit to the irregular-distance codes defined later.

The zero-rate threshold for adversarial channels is derived in [10]. Studying general channels, [10] deals with a broad notion of *confusability* between codewords. This is similar to the irregular distance codes in this work, however with the important distinction that here the confusability depends on the assignment between message vectors and codewords.

Codes that protect the output of a given machine learning algorithm against errors have been investigated in [11], [12], and [13]. While [11], [12] tailored their construction to optimize classification algorithms, [13] applied codes to the weights of the neurons in a neural network with the goal to optimize the output model of the neural network. These works prove that application-specific codes that protect the output of an algorithm against errors can outperform classical error-correcting codes. In principle, we follow a similar idea in this work, however the research in [11], [12], and [13] is specialized to specific classes of functions, while we discuss arbitrary functions. On the other hand, with the current state of research, it seems infeasible to practically and efficiently apply our generic results to such intricate functions.

We further would like to highlight the following works on error-correction within computations. Fourier stabilization has been used in [14] to increase the robustness of a neural network. Therein, error resilience was achieved by replacing the weights of neurons according to the solution of an associated combinatorial optimization problem. In [15], [16], and [17] computation in faulty dot-product engines is treated. While [15] and [16] construct codes over integers and real numbers that protect the computation of a matrix-vector product, [17] propose a theoretical framework for the error analysis of memristor crossbars. Codes that correct and detect errors in arithmetic operations are discussed in [18, ch.10].

C. Contributions

This paper builds a general theory for function-correction over adversarial channels. For arbitrary functions, we establish a connection between FCCs and *irregular-distance codes*. In particular, we show that the redundancy of an FCC is given by the shortest length of an irregular-distance code, which has a punctured pair-wise distance profile, which depends on the function. Deriving general lower and upper bounds on the optimal length of irregular distance codes, we obtain corresponding bounds on the optimal redundancy of FCCs for arbitrary functions. These results are applied to specific functions such as locally binary functions, the Hamming weight, the Hamming weight distribution, the min-max function and discretized real-valued functions. Finally, the redundancy of FCCs for specific functions is compared to schemes that use standard error-correcting codes. We restrict our attention to binary channels in this work, however most results can be generalized straightforwardly to larger alphabets. A summary of our quantitative results for specific functions is summarized and displayed in Table I.

D. Organization

Section II summarizes the problem considered and the main notations of the paper. Next, we study generic functions in Section III and reveal the fundamental connection between FCCs, irregular-distance codes, and independent sets in certain graphs. To this end, we show that the optimal redundancy of an FCC is equal to the smallest length of an irregular-distance code. We then provide simplified results that are easier to evaluate, especially for functions with entwined function regions. Further, generic converse and existential bounds on irregular-distance codes are presented. We then apply our generic results to specific functions in Sections IV, V, VI and VII. Section VIII concludes the paper.

II. Preliminaries

Let $\boldsymbol{u} \in \mathbb{Z}_2^k$ be the binary message and let $f : \mathbb{Z}_2^k \mapsto \mathsf{Im}(f) \triangleq \{f(\boldsymbol{u}) : \boldsymbol{u} \in \mathbb{Z}_2^k\}$ be a function computed on $\boldsymbol{u}$ with *expressiveness* $E \triangleq |\mathsf{Im}(f)| \leq 2^k$.[1] The message is encoded via the encoding function $\mathsf{Enc} : \mathbb{Z}_2^k \mapsto \mathbb{Z}_2^{k+r}$, $\mathsf{Enc}(\boldsymbol{u}) = (\boldsymbol{u}, \boldsymbol{p}(\boldsymbol{u}))$, where $\boldsymbol{p}(\boldsymbol{u}) \in \mathbb{Z}_2^r$ is the *redundancy vector* and r is the *redundancy*. The resulting codeword $\mathsf{Enc}(\boldsymbol{u})$ is transmitted over an erroneous channel, resulting in $\boldsymbol{y} \in \mathbb{Z}_2^{k+r}$ with $d(\mathsf{Enc}(\boldsymbol{u}), \boldsymbol{y}) \leq t$, where $d(\boldsymbol{x}, \boldsymbol{y})$ is the Hamming distance of $\boldsymbol{x}$ and $\boldsymbol{y}$. We define FCCs as follows.

Definition 1: An encoding function $\mathsf{Enc} : \mathbb{Z}_2^k \to \mathbb{Z}_2^{k+r}$ with $\mathsf{Enc}(\boldsymbol{u}) = (\boldsymbol{u}, \boldsymbol{p}(\boldsymbol{u}))$, $\boldsymbol{u} \in \mathbb{Z}_2^k$ defines a function-correcting code for the function $f : \mathbb{Z}_2^k \to \mathsf{Im}(f)$ if for all $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{Z}_2^k$ with $f(\boldsymbol{u}_1) \neq f(\boldsymbol{u}_2)$, it holds that

$$d(\mathsf{Enc}(\boldsymbol{u}_1), \mathsf{Enc}(\boldsymbol{u}_2)) \geq 2t + 1.$$

By this definition, given any $\boldsymbol{y}$, which is obtained by at most t errors from $\mathsf{Enc}(\boldsymbol{u})$, the receiver can uniquely recover $f(\boldsymbol{u})$, if it has knowledge about the function $f(\bullet)$ and the encoding function $\mathsf{Enc}(\bullet)$. Noteworthily, only codewords that originate from information vectors (messages) that evaluate to different function values need to have distance at least $2t+1$. Throughout the paper, a *standard error-correcting code* is an FCC for $f(\boldsymbol{u}) = \boldsymbol{u}$, i.e., a code that allows to reconstruct the whole message $\boldsymbol{u}$. We summarize some basic properties of FCCs in the following.

- For any bijective function f, any FCC is a standard error-correcting code.
- For any constant function f, the encoder $\mathsf{Enc}(\boldsymbol{u}) = \boldsymbol{u}$ is an FCC with redundancy 0.
- If the encoder has no knowledge about the function f, function-correction is only possible using standard error-correcting codes.

Note that the encoding and decoding complexity of FCCs may be higher or lower than that of standard error-correcting codes and heavily depends on the function f.

The main quantity of interest in this paper is the optimal redundancy of an FCC that is designed for a function f.

Definition 2: The optimal redundancy $r_f(k, t)$ is defined as the smallest r such that there exists an FCC with encoding function $\mathsf{Enc} : \mathbb{Z}_2^k \to \mathbb{Z}_2^{k+r}$ for the function f.

For any integer M, we write $[M]^+ \triangleq \max\{M, 0\}$ and we let $[M] \triangleq \{1, \ldots, M\}$. For a matrix $\boldsymbol{D}$, we denote by $[\boldsymbol{D}]_{ij}$ the (i, j)th entry of $\boldsymbol{D}$. For any two real numbers $a, b \in \mathbb{R}$, we define the closed and half-closed interval by $[a, b] \triangleq \{x \in \mathbb{R} : a \leq x \leq b\}$ and $[a, b) \triangleq \{x \in \mathbb{R} : a \leq x < b\}$. We denote by $\mathbb{N}_0$ the set of non-negative integers. Note that while our quantitative results in this paper are for substitution channels, the concepts can be generalized to other channels.

III. Generic Functions

This section is devoted to establishing general results on FCCs. We start by showing the equivalence of FCCs, irregular-distance codes (Definition 4), and independent sets[2] in an associated graph (Definition 5). We proceed afterwards with establishing several lower and upper bounds on the optimal redundancy of FCCs using these connections.

We begin with introducing irregular-distance codes. To this end, define the distance matrix of a function f as follows.

Definition 3: Let $\boldsymbol{u}_1, \ldots, \boldsymbol{u}_M \in \mathbb{Z}_2^k$. We define the distance requirement matrix $\boldsymbol{D}_f(t, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_M)$ of a function f as the $M \times M$ matrix with entries

$$[\boldsymbol{D}_f(t, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_M)]_{ij} = \begin{cases} [2t+1-d(\boldsymbol{u}_i, \boldsymbol{u}_j)]^+, & \text{if } f(\boldsymbol{u}_i) \neq f(\boldsymbol{u}_j), \\ 0, & \text{otherwise.} \end{cases}$$

Let $\mathcal{P} = \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_M\} \subseteq \mathbb{Z}_2^r$ be a code of length r and cardinality M. Here, we choose r as the code blocklength, as we will relate the code length r to the redundancy of FCCs later. Irregular-distance codes are formally defined as follows.

Definition 4: Let $\boldsymbol{D} \in \mathbb{N}_0^{M \times M}$. Then, $\mathcal{P} = \{\boldsymbol{p}_1, \boldsymbol{p}_2, \ldots, \boldsymbol{p}_M\}$ is a $\boldsymbol{D}$-code, if there exists an ordering of the codewords of $\mathcal{P}$ such that $d(\boldsymbol{p}_i, \boldsymbol{p}_j) \geq [\boldsymbol{D}]_{ij}$ for all $i, j \in [M]$.

Further, we define $N(\boldsymbol{D})$ to be the smallest integer r such that there exists a $\boldsymbol{D}$-code of length r. If $[\boldsymbol{D}]_{ij} = D$ for all $i \neq j$ we write $N(M, D)$.

With this definition, a $\boldsymbol{D}$-code requires individual distances between each pair of codewords.

Next, we define a function-dependent graph, whose independent sets, if large enough, form an FCC. The vertices constitute possible codewords of the FCC and we connect two vertices, if they can be contained together in an FCC.

Definition 5: We define $G_f(k, t, r)$ to be the graph with vertex set $V = \{0, 1\}^k \times \{0, 1\}^r$, such that each vertex has the form $\boldsymbol{x} = (\boldsymbol{u}, \boldsymbol{p}) \in \{0, 1\}^{k+r}$. Two vertices $\boldsymbol{x}_1 = (\boldsymbol{u}_1, \boldsymbol{p}_1)$ and $\boldsymbol{x}_2 = (\boldsymbol{u}_2, \boldsymbol{p}_2)$ are connected if $\boldsymbol{u}_1 = \boldsymbol{u}_2$ or both $f(\boldsymbol{u}_1) \neq f(\boldsymbol{u}_2)$ and $d(\boldsymbol{x}_1, \boldsymbol{x}_2) < 2t + 1$ hold.

We denote by $\gamma_f(k, t)$ the smallest integer r such that there exists an independent set of size 2^k in $G_f(k, t, r)$.
This graph resembles the characteristic graph in [9], however differs due to the fact that $\boldsymbol{u}$ is observed through the channel and that functions depend on the whole message vector in our problem formulation. Note that the edges between vertices with $\boldsymbol{u}_1 = \boldsymbol{u}_2$ enforce the property that each information vector $\boldsymbol{u}$ is assigned exactly one redundancy vector $\boldsymbol{p}(\boldsymbol{u})$. Fig. 2 visualizes the graph $G_f(k, t, r)$ and a corresponding FCC for a concrete example.

We find the following central connection between the redundancy of optimal FCCs, irregular-distance codes, and independent sets in the associated graphs.

Theorem 1 (): For any function $f : \mathbb{Z}_2^k \to \mathsf{Im}(f)$,

$$r_f(k, t) = \gamma_f(k, t) = N(\boldsymbol{D}_f(t, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{2^k})),$$

where $\{\boldsymbol{u}_1, \ldots, \boldsymbol{u}_{2^k}\} = \mathbb{Z}_2^k$ are all binary vectors of length k.

Proof: The first equality is immediate as an independent set in $G_f(k, t, r)$ exactly captures the required properties of an FCC. Further, the independent set has to have size 2^k such that there is one codeword for every message vector.

Next, we see that $r_f(k, t) \geq N(\boldsymbol{D}_f(t, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{2^k}))$ is necessary, as assuming to the contrary that $r_f(k, t) < N(\boldsymbol{D}_f(t, \boldsymbol{u}_1, \ldots, \boldsymbol{u}_{2^k}))$ implies that there must exist two redundancy vectors $\boldsymbol{p}_i$ and $\boldsymbol{p}_j$, $i \neq j$ with $d(\boldsymbol{p}_i, \boldsymbol{p}_j) < 2t +$

[1] The nature of the image $\mathsf{Im}(f)$, apart from its size, is not relevant in this paper. Thus, it is not further specified.

[2] An independent set of an undirected graph is a subset of vertices, where no two vertices are connected by an edge.

TABLE I

SUMMARY OF RESULTS ON THE OPTIMAL REDUNDANCY OF FCCS. THE ENTRIES MARKED WITH SUPERSCRIPT $*$ ARE APPROXIMATIONS FOR LARGE DATASET DIMENSIONS k AND EXPRESSIVENESS E (WHERE APPLICABLE), AND FIXED NUMBER OF ERRORS t, WHERE LOWER ORDER TERMS ARE NEGLECTED. THE REDUNDANCY OF FCCSIS DISPLAYED FOR THE CASE WHERE HADAMARD MATRICES OF CORRECT SIZE EXIST, CF. LEMMA 3. THESE RESTRICTIONS AND REGIMES ARE CHOSEN TO ALLOW FOR BETTER COMPARISON, HOWEVER OUR RESULTS ARE NOT RESTRICTED TO THESE REGIMES. PRECISE DEFINITIONS OF THE DISPLAYED FUNCTIONS CAN BE FOUND IN SECTION IV (BINARY AND LOCALLY BINARY), SECTION V-A (HAMMING WEIGHT), SECTION V-B (HAMMING WEIGHT DISTRIBUTION) AND SECTION VI (MIN-MAX). THE REDUNDANCIES *ECC on Data* AND *ECC on Function Values* ARE DERIVED IN APPENDIX A

Function	Parameters	Lower Bound	ECC on Data	ECC on Function Values	FCC
Binary	-	$2t$	$t\log k$ $*$	$2t+1$	$2t$
Locally binary	E	$2t$	$t\log k$ $*$	$\log E + t\log\log E$ $*$	$2t$
Hamming weight $\mathrm{wt}(\boldsymbol{u})$	-	$\frac{10}{3}(t-1)$	$t\log k$ $*$	$\log k + t\log\log k$ $*$	$4t$
Hamming weight distribution $\Delta_T(\boldsymbol{u})$	Threshold $T \geq 2t+1$, $E = \frac{k+1}{T}$	$2t$	$t\log k$ $*$	$\log E + t\log\log E$ $*$	$2t$
Min-max $\mathrm{mm}_w(\boldsymbol{u})$	Num. parts $w \gg 2t$	$2\log w +$ $(t-2)\log\log w$ $*$	$t\log k$ $*$	$2\log w + t\log\log w$ $*$	$2\log w +$ $t\log\log w$ $*$

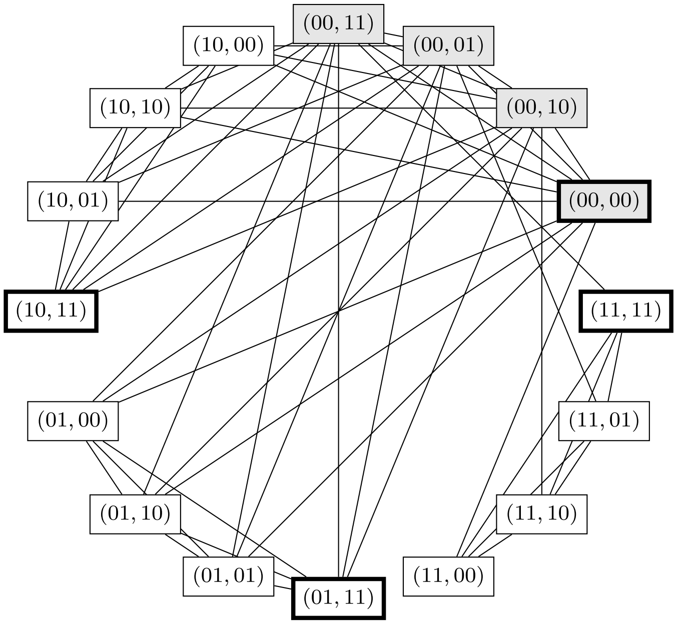


Fig. 2. Graph $G_f(k,t,r)$ for $k=2, t=1, r=2$, and the function $f((u_1,u_2)) = (u_1 \vee u_2)$. An independent set of size $2^k = 4$, i.e., an FCC for f, is highlighted in bold. The background colors highlight different function values.

$1 - d(\boldsymbol{u}_i,\boldsymbol{u}_j)$ and hence $d(\mathsf{Enc}(\boldsymbol{u}_i), \mathsf{Enc}(\boldsymbol{u}_j)) = d(\boldsymbol{u}_i,\boldsymbol{u}_j) + d(\boldsymbol{p}_i,\boldsymbol{p}_j) < 2t+1$, which contradicts Definition 1.

On the other hand $r_f(k,t) \leq N(\boldsymbol{D}_f(t,\boldsymbol{u}_1,\ldots,\boldsymbol{u}_{2^k}))$, as using a correctly assigned $\boldsymbol{D}_f(t,\boldsymbol{u}_1,\ldots,\boldsymbol{u}_{2^k})$-code for the redundancy vectors gives an FCC. □

Remark 1: The irregularity of the distance profile of FCCs comes from imposing distance constraints on the redundancy vectors as opposed to codewords. In our analysis, we found this approach to naturally capture the interplay between the message and the redundancy part and to help with the derivation of simplified bounds and constructions, which are presented in the sequel.

With the result of Theorem 1, one can deduce insights into FCCs using known results about the sizes of independent sets in general graphs, such as [19] and [20].

However, the problem of finding *optimal* FCCs requires the determination of whether the size of the largest independent set meets the threshold 2^k. The related problem of finding a maximal independent set in arbitrary graphs is known to be NP-complete [21], which indicates that also the problem of finding optimal FCCs is complex, unless the structure of the analyzed function f imposes an easily tractable graph structure that simplifies the search for large independent sets.

This implies that the construction of optimal FCCs may become computationally infeasible for large parameters and unstructured functions. To cope with such scenarios, we derive simplified, possibly sub-optimal, results on irregular-distance codes, in order to facilitate the research for arbitrary functions. We proceed with deriving results that act on a smaller set of information vectors and ease the derivation of analytical results.

A. Simplified Redundancy Lower Bounds

We first compute simplified lower bounds on the optimal redundancy of FCCs. Using an arbitrary subset of information vectors $\boldsymbol{u}_1,\ldots,\boldsymbol{u}_M$ with $M \leq 2^k$ we can obtain a lower bound on the redundancy as follows.

Corollary 1: Let $\boldsymbol{u}_1,\ldots,\boldsymbol{u}_M \in \mathbb{Z}_2^k$ be arbitrary different vectors. Then, the redundancy of an FCC is at least

$$r_f(k,t) \geq N(\boldsymbol{D}_f(t,\boldsymbol{u}_1,\ldots,\boldsymbol{u}_M)).$$

For any function f with $|\mathsf{Im}(f)| \geq 2$,

$$r_f(k,t) \geq 2t.$$

Proof: The first statement is immediate, since any subset of information vectors must also fulfill the FCC conditions.

Since $|\mathsf{Im}(f)| \geq 2$, there exist $\boldsymbol{u},\boldsymbol{u}' \in \mathbb{Z}_2^k$ with $d(\boldsymbol{u},\boldsymbol{u}') = 1$ and $f(\boldsymbol{u}) \neq f(\boldsymbol{u}')$. It follows that $r_f(k,t) \geq N(2,2t)$.

Further, $N(2,2t) = 2t$, which is attained by the repetition code $\mathcal{P} = \{(0,\dots,0),(1,\dots,1)\}$ of length $2t$. □

Finding $N(\boldsymbol{D}_f(t,\boldsymbol{u}_1,\dots,\boldsymbol{u}_{2^k}))$ is in general quite difficult and it can be easier to focus only on a small but representative subset of information vectors. However, the particular subset heavily depends on the function itself and it is not possible to give a generic approach on how a good subset can be found. Loosely speaking, good bounds are obtained for information vectors that have distinct function values and are close in Hamming distance. Throughout this paper, we will provide some insights on good choices of information vectors using illustrative examples.

B. Simplified Existential Bounds

We proceed with simplifying Theorem 1 in order to obtain easier computable existential bounds. We start by defining the distance between two function values.

Definition 6: The distance between two function values $f_1, f_2 \in \mathsf{Im}(f)$ is defined as the smallest distance between two information vectors that evaluate to f_1 and f_2, i.e.,

$$d_f(f_1,f_2) \triangleq \min_{\boldsymbol{u}_1,\boldsymbol{u}_2\in\mathbb{Z}_2^k} d(\boldsymbol{u}_1,\boldsymbol{u}_2) \text{ s.t. } f(\boldsymbol{u}_1)=f_1 \wedge f(\boldsymbol{u}_2)=f_2.$$

Note that the distance $d_f(f_1,f_1) = 0, \forall f_1 \in \mathsf{Im}(f)$. The function-distance matrix of f is thus defined as follows.

Definition 7: The function-distance matrix of a function f is denoted by the $E \times E$ matrix $\boldsymbol{D}_f(t,f_1,\dots,f_E)$ with entries $[\boldsymbol{D}_f(t,f_1,\dots,f_E)]_{ij} = [2t+1-d_f(f_i,f_j)]^+$, if $i \neq j$ and $[\boldsymbol{D}_f(t,f_1,\dots,f_E)]_{ii} = 0$.

One way to construct FCCs is to assign the same redundancy vector to all information vectors $\boldsymbol{u}$ that evaluate to the same function value. This is not a necessity, however it gives rise to the following existence theorem.

Theorem 2: For any arbitrary function $f : \mathbb{Z}_2^k \to \mathsf{Im}(f)$,

$$r_f(k,t) \le N(\boldsymbol{D}_f(t,f_1,\dots,f_E)).$$

Proof: We describe how to construct an FCC. The redundancy vectors are chosen to depend only on the function value of $\boldsymbol{u}$, i.e., the encoding mapping is defined by $\boldsymbol{u} \mapsto (\boldsymbol{u},\boldsymbol{p}(f(\boldsymbol{u})))$. Denote by $\boldsymbol{p}_i$ the redundancy vector assigned to all $\boldsymbol{u}$ with $f(\boldsymbol{u}) = f_i$. Therefore, two information vectors with the same function value have the same redundancy vectors. We then choose $\boldsymbol{p}_1,\dots,\boldsymbol{p}_E$ such that $d(\boldsymbol{p}_i,\boldsymbol{p}_j) \ge 2t+1-d_f(f_i,f_j)$. It follows that for any $\boldsymbol{u}_i,\boldsymbol{u}_j$ with $f(\boldsymbol{u}_i) = f_i$, $f(\boldsymbol{u}_j) = f_j$, $f_i \neq f_j$, we have $d(\mathsf{Enc}(\boldsymbol{u}_i),\mathsf{Enc}(\boldsymbol{u}_j)) = d(\boldsymbol{u}_i,\boldsymbol{u}_j) + d(\boldsymbol{p}_i,\boldsymbol{p}_j) \ge d_f(f_i,f_j) + 2t+1-d_f(f_i,f_j) = 2t+1$. By Definition 4 we can guarantee the existence of such parity vectors $\boldsymbol{p}_1,\dots,\boldsymbol{p}_E$, if they have length $N(\boldsymbol{D}_f(t,f_1,\dots,f_E))$. □

There are cases in which the bound in Theorem 2 is tight. We characterize one important case in the following corollary, which is a consequence of Corollary 1 and Theorem 2.

Corollary 2: If there exists a set of representative information vectors $\boldsymbol{u}_1,\dots,\boldsymbol{u}_E$ with $\{f(\boldsymbol{u}_1),\dots,f(\boldsymbol{u}_E)\} = \mathsf{Im}(f)$ and $\boldsymbol{D}_f(t,\boldsymbol{u}_1,\dots,\boldsymbol{u}_E) = \boldsymbol{D}_f(t,f_1,\dots,f_E)$, then

$$r_f(k,t) = N(\boldsymbol{D}_f(t,f_1,\dots,f_E)).$$

Even though the bound in Theorem 2 is not necessarily tight, in many cases it is much easier to derive the function distance matrix $\boldsymbol{D}_f(t,f_1,\dots,f_E)$ than the distance requirement matrix $\boldsymbol{D}_f(t,\boldsymbol{u}_1,\dots,\boldsymbol{u}_{2^k})$ and the corresponding value $N(\boldsymbol{D}_f(t,f_1,\dots,f_E))$, especially when E is small.

C. Irregular-Distance Codes

We summarize some results about $N(\boldsymbol{D})$ here, which allow us to obtain results on the redundancy of FCCs using Theorems 1 and 2. We start with a generalization of the Plotkin bound [22] on codes with irregular distance requirements.

Lemma 1: For any distance matrix $\boldsymbol{D} \in \mathbb{N}_0^{M\times M}$,

$$N(\boldsymbol{D}) \ge \begin{cases} \frac{4}{M^2}\sum\limits_{i,j:i<j}[\boldsymbol{D}]_{ij}, & \text{if } M \text{ is even,} \\ \frac{4}{M^2-1}\sum\limits_{i,j:i<j}[\boldsymbol{D}]_{ij}, & \text{if } M \text{ is odd.} \end{cases}$$

Proof: We start by proving the statement for M even. Let $\boldsymbol{p}_1,\dots,\boldsymbol{p}_M$ be codewords of a $\boldsymbol{D}$-code of length r. Stack these codewords as rows of a matrix $\boldsymbol{P}$. Since each column of the matrix $\boldsymbol{P}$ can contribute at most $\frac{M^2}{4}$ to the sum $\sum_{i,j:i<j} d(\boldsymbol{p}_i,\boldsymbol{p}_j)$ (when the weight of the column is exactly $\frac{M}{2}$), we have that $\sum_{i,j:i<j} d(\boldsymbol{p}_i,\boldsymbol{p}_j) \le r\frac{M^2}{4}$. On the other hand, by the definition of a $\boldsymbol{D}$-code, $d(\boldsymbol{p}_i,\boldsymbol{p}_j) \ge [\boldsymbol{D}]_{ij}$ and the statement follows. The statement for odd M is proven accordingly using the fact that in this case the maximum contribution of a column is $\frac{M+1}{2}\frac{M-1}{2}$. □

For the case of regular-distance codes with minimum distance D, Lemma 1 implies $N(M,D) \ge 2D\frac{M-1}{M}$, a variant of Plotkin's bound. Conversely, we can derive an achievability bound, which is a generalization of the well-known Gilbert-Varshamov bound [23], [24] to irregular-distance codes. To this end we define $V(r,d) = \sum_{i=0}^{d}\binom{r}{i}$ as the size of the binary radius-d Hamming sphere over vectors of length r.

Lemma 2: For any distance matrix $\boldsymbol{D} \in \mathbb{N}_0^{M\times M}$, and any permutation $\pi : [M] \to [M]$

$$N(\boldsymbol{D}) \le \min_{r\in\mathbb{N}}\left\{ r : 2^r > \max_{j\in[M]}\sum_{i=1}^{j-1} V(r,[\boldsymbol{D}]_{\pi(i)\pi(j)}-1)\right\}.$$

Proof: We describe how to construct a code of length r meeting the distance requirements by iteratively selecting valid codewords. Assume first for simplicity that $\pi(i) = i$. Start by choosing an arbitrary codeword $\boldsymbol{p}_1 \in \mathbb{Z}_2^r$. Then, choose a valid codeword $\boldsymbol{p}_2$ as follows. Since the distance of $\boldsymbol{p}_1$ and $\boldsymbol{p}_2$ needs to be at least $[\boldsymbol{D}]_{12}$, we choose an arbitrary $\boldsymbol{p}_2$ such that $d(\boldsymbol{p}_1,\boldsymbol{p}_2) \ge [\boldsymbol{D}]_{12}$. Such a codeword $\boldsymbol{p}_2$ exists, if the length satisfies $2^r > V(r,[\boldsymbol{D}]_{12}-1)$. Next, we choose the third codeword $\boldsymbol{p}_3$. Similarly as before, we need to have $d(\boldsymbol{p}_1,\boldsymbol{p}_3) \ge [\boldsymbol{D}]_{13}$ and also $d(\boldsymbol{p}_2,\boldsymbol{p}_3) \ge [\boldsymbol{D}]_{23}$. If $2^r > V(r,[\boldsymbol{D}]_{13}-1)+V(r,[\boldsymbol{D}]_{23}-1)$ we can guarantee the existence of such a codeword $\boldsymbol{p}_3$. The theorem then follows by iteratively selecting the remaining codewords $\boldsymbol{p}_j$ such that $d(\boldsymbol{p}_i,\boldsymbol{p}_j) \ge [\boldsymbol{D}]_{ij}$ for all $i < j$. Under the condition of the theorem, we can guarantee existence of all codewords. Since the codewords can be chosen in an arbitrary order, the lemma holds for any order π in which the codewords are selected. □

Note that for codes with $[\boldsymbol{D}]_{ij} = D$, this bound results in the well-known Gilbert-Varshamov bound [23], [24].

Several of our results in the following require codes of small cardinality, i.e., the code size is in the same order of magnitude as the minimum distance. The following result is based on Hadamard codes [25], [26].

Lemma 3 (cf. [26, Def.3.13]): Let $D \in \mathbb{N}$ be such that there exists a Hadamard matrix of order D and $M \leq 4D$. Then,

$$N(M, D) \leq 2D.$$

The range of the parameter D is restricted to the limited knowledge of lengths for which Hadamard codes exist. Note that there exist other good codes of small size, such as weak flip codes [27], however, they only attain the Plotkin bound for a limited range of parameters. In general, it is possible to puncture or juxtapose Hadamard codes (cf. Levenshtein's theorem [25, Section2.3]) to obtain codes for a larger range of parameters. However, for our discussion, the application of the Gilbert-Varshamov bound is sufficient and further allows to prove the existence of codes whose size is quadratic in their minimum distance as follows.

Lemma 4: For any $M, D \in \mathbb{N}$ with $D \geq 10$ and $M \leq D^2$,

$$N(M, D) \leq \frac{2D}{1 - 2\sqrt{\ln(D)/D}}.$$

The proof of Lemma 4 is obtained using Lemma 2 together with [28, Lemma4.7.2] and is presented in Appendix B. This result means that, given that the size of the code is moderate, i.e., $M \leq D^2$, for large D, the optimal length of an error-correcting code approaches $2D$. While Lemma 4 gives a slightly weaker bound than Lemma 3, it holds for any D and for larger code sizes M. Note that a similar bound as in Lemma 4 can easily be derived also for larger M, i.e., $M \leq D^m$, $m > 2$, however $m = 2$ is sufficient for the subsequent analysis. Denoting $D_{\max} = \max_{i,j}[\boldsymbol{D}]_{ij}$, with these bounds it is immediate that, if $M \leq D_{\max}^2$, it holds that $D_{\max} \leq N(\boldsymbol{D}) \leq 2D_{\max}/(1 - 2\sqrt{\ln(D_{\max})/D_{\max}})$.

In the following sections, we turn to discuss specific functions and give bounds on their optimal redundancy, which are tight in several cases. For several instances we additionally give explicit code constructions that can be encoded efficiently. The functions under discussion are locally binary functions, the Hamming weight function, the Hamming weight distribution function, the min-max function and a collection of discretized real-valued functions.

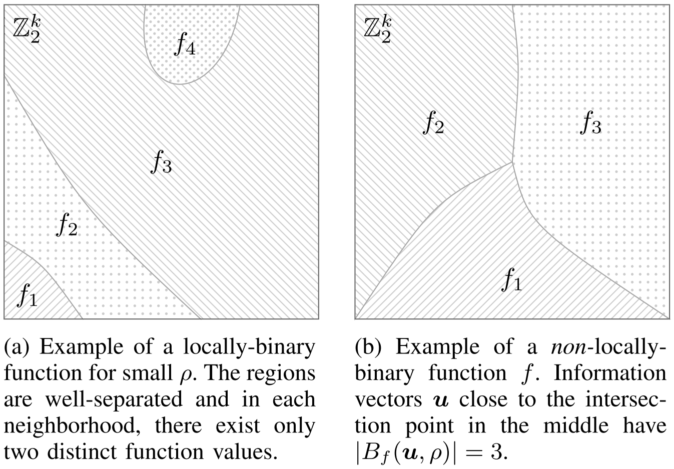
IV. Locally Binary Functions

In the following we define a broad class of functions, called locally binary functions. We derive their optimal redundancy and show how it can be obtained using a simple explicit code construction. This class of functions is defined next.

Definition 8: The function ball of a function f with radius ρ around $\boldsymbol{u} \in \mathbb{Z}_2^k$ is defined by

$$B_f(\boldsymbol{u}, \rho) = \{f(\boldsymbol{u}') : \boldsymbol{u}' \in \mathbb{Z}_2^k \wedge d(\boldsymbol{u}, \boldsymbol{u}') \leq \rho\}.$$

Locally binary functions are defined as follows.



(a) Example of a locally-binary function for small ρ. The regions are well-separated and in each neighborhood, there exist only two distinct function values.

(b) Example of a *non*-locally-binary function f. Information vectors $\boldsymbol{u}$ close to the intersection point in the middle have $|B_f(\boldsymbol{u}, \rho)| = 3$.

Fig. 3. Visualization of (non-)locally binary functions. Shaded areas highlight function regions, i.e., $\{\boldsymbol{u} \in \mathbb{Z}_2^k : f(\boldsymbol{u}) = f_i\}$.

Definition 9: A function $f : \mathbb{Z}_2^k \to \mathsf{Im}(f)$ is called a ρ-locally binary function, if for all $\boldsymbol{u} \in \mathbb{Z}_2^k$,

$$|B_f(\boldsymbol{u}, \rho)| \leq 2.$$

Intuitively, a ρ-locally binary function is a function, where the function regions of all function values are well spread in the sense that each information word is close to only one region of another function value, see Fig. 3. Note that by this definition, any binary function, i.e., $|\mathsf{Im}(f)| = 2$, is also a ρ-locally binary function for arbitrary ρ. We can directly prove the following optimality.

Lemma 5: For any $2t$-locally binary function f,

$$r_f(k, t) = 2t.$$

Proof: By Corollary 1, $r_f(k, t) \geq 2t$. On the other hand, we can prove achievability using the following explicit code construction. Let $\mathsf{Im}(f) = \{f_1, \ldots, f_E\}$ and set w.l.o.g. $f_i \triangleq i$. Let $\boldsymbol{u}$ be the information word to be encoded and define the following function,

$$\omega_{2t}(\boldsymbol{u}) = \begin{cases} 1, & \text{if } \ f(\boldsymbol{u}) = \max B_f(\boldsymbol{u}, 2t), \\ 0, & \text{otherwise.} \end{cases}$$

Now, use $\mathsf{Enc}(\boldsymbol{u}) = (\boldsymbol{u}, (\omega_{2t}(\boldsymbol{u}))^{2t})$, i.e. the $2t$-fold repetition of the bit $\omega_{2t}(\boldsymbol{u})$. This gives an FCC for the function f due to the following. Assume $(\boldsymbol{u}, \boldsymbol{p}) = \mathsf{Enc}(\boldsymbol{u})$ has been transmitted and $(\boldsymbol{u}', \boldsymbol{p}')$ has been received. The decoder first computes $B_f(\boldsymbol{u}', t)$. Notice that $f(\boldsymbol{u}) \in B_f(\boldsymbol{u}', t) \subseteq B_f(\boldsymbol{u}, 2t)$. If $|B_f(\boldsymbol{u}', t)| = 1$, then it trivially contains the correct function value $f(\boldsymbol{u})$. Otherwise, $B_f(\boldsymbol{u}', t) = B_f(\boldsymbol{u}, 2t)$, since $|B_f(\boldsymbol{u}', t)| > 1$ and, by the definition of $2t$-locally binary functions, $|B_f(\boldsymbol{u}, 2t)| \leq 2$. The decoder performs a majority decision over the $2t+1$ bits $(\omega_{2t}(\boldsymbol{u}'), \boldsymbol{p}')$ and obtains correctly $\omega_{2t}(\boldsymbol{u})$, as at most t out of these $2t + 1$ bits are erroneous. Finally, the receiver decides for $\max B_f(\boldsymbol{u}', t)$, if $\omega_{2t}(\boldsymbol{u}) = 1$ and for $\min B_f(\boldsymbol{u}', t)$, otherwise. □

It is noteworthy that the code construction used in Lemma 5 leverages the side information provided by the message $\boldsymbol{u}$ using $\omega_{2t}(\boldsymbol{u}')$ for decoding, which allows to achieve a redundancy of only $2t$. This side information is particularly useful for locally binary functions due to the structured topology of the function regions, which is visualized in Fig. 3. Ignoring this side information would require significantly more redundancy, cf. Table I.

In Section V-B we will present an explicit example of a locally binary function. For illustration, another example of a locally binary function is presented in the following.

Example 1: Assume the codewords $\mathcal{Q} = \{\mathbf{q}_1, \ldots, \mathbf{q}_N\} \subseteq \mathbb{Z}_2^k$ form a code of length k with minimum distance $d = \min_{i \neq j} d(\mathbf{q}_i, \mathbf{q}_j)$. Then the indicator function

$$\mathbb{I}_{\mathcal{Q}}(\boldsymbol{u}) = \begin{cases} i, & \text{if } \boldsymbol{u} = \mathbf{q}_i, \\ 0, & \text{otherwise} \end{cases}$$

is $\lfloor \frac{d-1}{2} \rfloor$-locally binary.

V. Functions Based on the Hamming Weight

In this section we study two functions: the Hamming weight function $f(\boldsymbol{u}) = \mathrm{wt}(\boldsymbol{u})$ and the Hamming weight distribution function $f(\boldsymbol{u}) = \Delta_T(\boldsymbol{u}) = \lfloor \frac{\mathrm{wt}(\boldsymbol{u})}{T} \rfloor$, for a given threshold T.

A. Hamming Weight Function

Let $f(\boldsymbol{u}) = \mathrm{wt}(\boldsymbol{u})$, where $\boldsymbol{u} \in \mathbb{Z}_2^k$. Note that the expressiveness of $\mathrm{wt}(\bullet)$ is $E = |\mathsf{Im}(\mathrm{wt})| = k + 1$. We start by showing that for this function it is possible to achieve optimal redundancy by an encoding function which only depends on the function value, i.e., the Hamming weight of $\boldsymbol{u}$. Throughout this section we refer to the function distance matrix $\boldsymbol{D}_{\mathrm{wt}}(t, f_1, \ldots, f_E)$ as $\boldsymbol{D}_{\mathrm{wt}}(t)$ for ease of notation.

Lemma 6: Let $f(\boldsymbol{u}) = \mathrm{wt}(\boldsymbol{u})$. Consider the $(k+1) \times (k+1)$ matrix $\boldsymbol{D}_{\mathrm{wt}}(t)$ with entries $[\boldsymbol{D}_{\mathrm{wt}}(t)]_{ii} = 0$ and $[\boldsymbol{D}_{\mathrm{wt}}(t)]_{ij} = [2t + 1 - |i - j|]^+$ for $i \neq j$. Then,

$$r_{\mathrm{wt}}(k, t) = N(\boldsymbol{D}_{\mathrm{wt}}(t)).$$

Proof: The function values of the Hamming weight function belong to $\mathsf{Im}(\mathrm{wt}) = \{0, 1, \ldots, k\}$ and we let $i, j \in \{0, 1, \ldots, k\}$ denote two function values. First, we see that the function distance is given by $d_{\mathrm{wt}}(i, j) = |i - j|$, since

$$\min_{\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{Z}_2^k} d(\boldsymbol{u}_1, \boldsymbol{u}_2) \text{ s.t. } \mathrm{wt}(\boldsymbol{u}_1) = i, \mathrm{wt}(\boldsymbol{u}_2) = j$$

is equal to $|i - j|$. It follows from Theorem 2 that $r_{\mathrm{wt}}(k, t) \leq N(\boldsymbol{D}_{\mathrm{wt}}(t))$. On the other hand, using $\boldsymbol{u}_i = (1^i 0^{k-i})$, $i \in \{0, 1, \ldots, k\}$, we see that $\mathrm{wt}(\boldsymbol{u}_i) = i$ and their pairwise distances are $d(\boldsymbol{u}_i, \boldsymbol{u}_j) = |i - j|$. We can then apply Corollary 1 to obtain $r_{\mathrm{wt}}(k, t) \geq N(\boldsymbol{D}_{\mathrm{wt}}(t))$. □

The following example visualizes the general structure of the function distance matrix $\boldsymbol{D}_{\mathrm{wt}}(t)$.

Example 2: The function distance matrix $\boldsymbol{D}_{\mathrm{wt}}(2)$ for $k = 6$ is given by the symmetric 7×7 matrix with entries

$$\boldsymbol{D}_{\mathrm{wt}}(2) = \begin{array}{c|ccccccc} \mathrm{f}(\boldsymbol{u}) & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 0 & 0 & 4 & 3 & 2 & 1 & 0 & 0 \\ 1 & 4 & 0 & 4 & 3 & 2 & 1 & 0 \\ 2 & 3 & 4 & 0 & 4 & 3 & 2 & 1 \\ 3 & 2 & 3 & 4 & 0 & 4 & 3 & 2 \\ 4 & 1 & 2 & 3 & 4 & 0 & 4 & 3 \\ 5 & 0 & 1 & 2 & 3 & 4 & 0 & 4 \\ 6 & 0 & 0 & 1 & 2 & 3 & 4 & 0 \end{array}.$$

Based on Lemma 6, we can infer a lower bound on the redundancy using the Plotkin-like bound of Lemma 1.

Corollary 3: For any $k > t$,

$$r_{\mathrm{wt}}(k, t) \geq \frac{10t^3 + 30t^2 + 20t + 12}{3t^2 + 12t + 12}.$$

Proof: Let $\{\boldsymbol{p}_1, \ldots, \boldsymbol{p}_{k+1}\}$ be a $\boldsymbol{D}_{\mathrm{wt}}(t)$-code. We will prove the corollary by applying the Plotkin-type bound on a subcode of $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_{k+1}$. Consider the first $t + 2$ codewords $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_{t+2}$. By Lemma 6, we have that $[\boldsymbol{D}_{\mathrm{wt}}(t)]_{ij} = 2t + 1 - |i - j|$ and thus $[\boldsymbol{D}_{\mathrm{wt}}(t)]_{12} + [\boldsymbol{D}_{\mathrm{wt}}(t)]_{13} + [\boldsymbol{D}_{\mathrm{wt}}(t)]_{23} = 6t - 1$. However, since $d(\boldsymbol{p}_1, \boldsymbol{p}_2) + d(\boldsymbol{p}_1, \boldsymbol{p}_3) + d(\boldsymbol{p}_2, \boldsymbol{p}_3)$ must be an even value, it follows that $d(\boldsymbol{p}_1, \boldsymbol{p}_2) + d(\boldsymbol{p}_1, \boldsymbol{p}_3) + d(\boldsymbol{p}_2, \boldsymbol{p}_3) \geq 6t$. With this strengthened bound, the sum of the pairwise distances in Lemma 1 can be increased by one and we obtain

$$\begin{aligned} r_{\mathrm{wt}}(k, t) &\overset{(a)}{\geq} \frac{4}{(t+2)^2} \left(1 + \sum_{i=1}^{t+2} \sum_{j=i+1}^{t+2} [\boldsymbol{D}_{\mathrm{wt}}(t)]_{ij} \right) \\ &\overset{(b)}{=} \frac{4}{(t+2)^2} \left(1 + \sum_{i=0}^{t} (t + 1 - i)(2t - i) \right) \\ &= \frac{10t^3 + 30t^2 + 20t + 12}{3t^2 + 12t + 12}. \end{aligned}$$

Hereby, inequality (a) follows from Lemma 1, with an additional summand of 1 due to the fact that $d(\boldsymbol{p}_1, \boldsymbol{p}_2) + d(\boldsymbol{p}_1, \boldsymbol{p}_3) + d(\boldsymbol{p}_2, \boldsymbol{p}_3)$ must be even, as explained above. Eq. (b) follows from summing over the diagonals of $\boldsymbol{D}_{\mathrm{wt}}(t)$. □

For the following results, we require the *shifted* modulo function, which is defined as follows.

Definition 10: We define the shifted modulo operator by

$$a \text{ smod } b \triangleq ((a - 1) \bmod b) + 1 \in \{1, 2, \ldots, b\}.$$

E.g., $(3 \text{ smod } 3) = 3$ and $(4 \text{ smod } 3) = 1$. We now describe a construction of an FCC for the function $\mathrm{wt}(\boldsymbol{u})$.

Construction 1: We define

$$\mathsf{Enc}_{\mathrm{wt}}(\boldsymbol{u}) = (\boldsymbol{u}, \boldsymbol{p}_{\mathrm{wt}(\boldsymbol{u})+1}),$$

where the $\boldsymbol{p}_i$'s are defined depending on t as follows.

For $t = 1$, set $\boldsymbol{p}_1 = (000)$, $\boldsymbol{p}_2 = (110)$ and $\boldsymbol{p}_3 = (011)$. Then set $\boldsymbol{p}_i = \boldsymbol{p}_{i \text{ smod } 3}$ for $i \geq 4$.

For $t = 2$ set $\boldsymbol{p}_1 = (000000)$, $\boldsymbol{p}_2 = (110011)$, $\boldsymbol{p}_3 = (001111)$, $\boldsymbol{p}_4 = (111100)$. Then set $\boldsymbol{p}_i = \boldsymbol{p}_{i-4} + (000001)$ for $i \in \{5, 6, 7, 8\}$ and $\boldsymbol{p}_i = \boldsymbol{p}_{i \text{ smod } 8}$ for $i \geq 9$.

For $t \geq 3$, let $\boldsymbol{p}_1, \ldots, \boldsymbol{p}_{2t+1}$ be a code with minimum distance $2t$, i.e., $d(\boldsymbol{p}_i, \boldsymbol{p}_j) \geq 2t$ for all $i, j \leq 2t + 1$, $i \neq j$ and set $\boldsymbol{p}_i = \boldsymbol{p}_{i \text{ smod } (2t+1)}$ for $i \geq 2t + 2$.

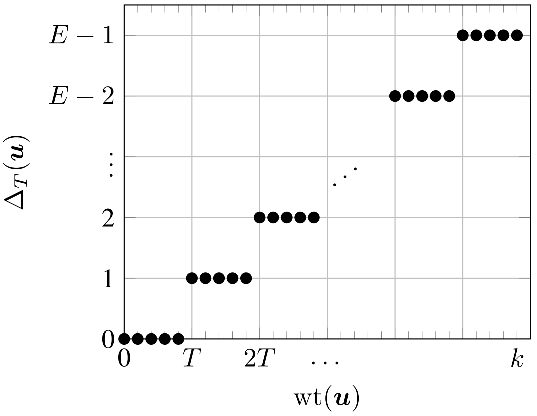


Fig. 4. Illustration of the Hamming weight distribution function with step size $T = \frac{k+1}{E}$.

We can use Corollary 3 to narrow down the optimal redundancy of FCCs for the Hamming weight function as follows.

Lemma 7: For any $k > 2$, $r_{\mathrm{wt}}(k, 1) = 3$ and $r_{\mathrm{wt}}(k, 2) = 6$. Further, for $t \geq 5$ and $k > t$,

$$\frac{10t}{3} - \frac{10}{3} \leq r_{\mathrm{wt}}(k,t) \leq \frac{4t}{1 - 2\sqrt{\ln(2t)/(2t)}}.$$

Proof: We start with the case $t = 1$. It is quickly verified that $d(\boldsymbol{p}_i, \boldsymbol{p}_j) \geq [\boldsymbol{D}_{\mathrm{wt}}(1)]_{ij}$ for all $i \neq j$, $i, j \leq k+1$ and thus giving a valid FCC. Further, Corollary 3 gives $r_{\mathrm{wt}}(k, 1) \geq 3$. For the case $t = 2$, it can be verified that $d(\boldsymbol{p}_i, \boldsymbol{p}_j) \geq [\boldsymbol{D}_{\mathrm{wt}}(2)]_{ij}$. Again, Corollary 3 gives $r_{\mathrm{wt}}(k, 1) \geq 6$, proving optimality of the proposed code. For $t \geq 3$, we obtain $d(\boldsymbol{p}_i, \boldsymbol{p}_j) \geq [\boldsymbol{D}_{\mathrm{wt}}(t)]_{ij}$ as desired. The lower and upper bound on $r_{\mathrm{wt}}(k, t)$ follow from Corollary 3 and Lemma 4. □

Recall here that using a standard error-correcting code with minimum distance $2t + 1$, e.g., a BCH code, results in a redundancy of roughly $t \log k$. Therefore, using FCCs, we can improve the scaling of the redundancy by a factor of $\log k$. While we find the optimal redundancy exactly for $t = 1$ and $t = 2$, there is still a gap for $t \geq 3$ narrowing down the optimal redundancy between roughly $\frac{10t}{3}$ and $4t$.

B. Hamming Weight Distribution Function

Let in the following $T \in \mathbb{N}$ be a parameter of choice. For simplicity, we restrict T to divide $k+1$. Consider the function $f(\boldsymbol{u}) = \Delta_T(\boldsymbol{u}) \triangleq \lfloor \frac{\mathrm{wt}(\boldsymbol{u})}{T} \rfloor$. We directly see that the number of distinct function values is equal to $E = \frac{k+1}{T}$. This function defines a step threshold function, based on the Hamming weight of $\boldsymbol{u}$, with $E-1$ steps. The threshold values, where the function values increase by one, are at integer multiples of T, see Fig. 4. We restrict to the case where $2t+1 \leq T$ and will give an optimal construction with redundancy $r_{\Delta_T}(k, t) = 2t$ in this regime. First, note that, when $4t+1 \leq T$, we can show that $\Delta_T(\boldsymbol{u})$ is $2t$-locally binary, as two consecutive thresholds have distance at least $4t + 1$. Consequently, $r_{\Delta_T}(k, t) = 2t$ by Lemma 5. We now focus on the more general case, where $2t + 1 \leq T$. We start by describing the encoding function. Recall the shifted modulo operation from Definition 10.

TABLE II
PARITY VECTORS OF THE HAMMING WEIGHT DISTRIBUTION FUNCTION FOR $T = 2t + 1$

$\mathrm{wt}(\boldsymbol{u})$	$\boldsymbol{p}_{\mathrm{wt}(\boldsymbol{u})+1}$	$f(\boldsymbol{u})$
$mT - T$	$(000\ldots000)$	$m-1$
$mT - T + 1$	$(100\ldots000)$	
$\vdots$	$\vdots$	
$mT - 2$	$(111\ldots110)$	
$mT - 1$	$(111\ldots111)$	
mT	$(000\ldots000)$	m
$mT + 1$	$(100\ldots000)$	
$\vdots$	$\vdots$	

Construction 2: We define

$$\mathsf{Enc}_{\Delta_T}(\boldsymbol{u}) = (\boldsymbol{u}, \boldsymbol{p}_{\mathrm{wt}(\boldsymbol{u})}),$$

with $\boldsymbol{p}_i \in \mathbb{Z}_2^{2t}$ defined as follows. Set $\boldsymbol{p}_i = (1^{i-1}0^{2t-i+1})$ for $i \in [2t+1]$, $\boldsymbol{p}_i = (1^{2t})$ for $i \in \{2t+2, \ldots, T\}$ and $\boldsymbol{p}_i = \boldsymbol{p}_{i \text{ smod } T}$, if $i \geq T+1$.
We show that this encoding function gives an FCC for the Hamming weight distribution function $\Delta_T(\boldsymbol{u})$.

Lemma 8: For any $k, t, T \in \mathbb{N}$ such that T divides $(k+1)$ and $2t+1 \leq T$,

$$r_{\Delta_T}(k, t) = 2t.$$

Proof: By Corollary 1, $r_{\Delta_T}(k, t) \geq 2t$. We now argue that Construction 2 is an FCC of redundancy $2t$ by showing that $d(\mathsf{Enc}_{\Delta_T}(\boldsymbol{u}_1), \mathsf{Enc}_{\Delta_T}(\boldsymbol{u}_2)) \geq 2t+1$ for all $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{Z}_2^k$ with $f(\boldsymbol{u}_1) \neq f(\boldsymbol{u}_2)$. Let $\boldsymbol{u}_1, \boldsymbol{u}_2 \in \mathbb{Z}_2^k$ with $f(\boldsymbol{u}_1) \neq f(\boldsymbol{u}_2)$ be two information vectors that evaluate to two different function values. Note that, if $d(\boldsymbol{u}_1, \boldsymbol{u}_2) \geq 2t+1$, we automatically have $d(\mathsf{Enc}_{\Delta_T}(\boldsymbol{u}_1), \mathsf{Enc}_{\Delta_T}(\boldsymbol{u}_2)) \geq 2t+1$ and we therefore restrict to the interesting case $d(\boldsymbol{u}_1, \boldsymbol{u}_2) < 2t+1$. Since $f(\boldsymbol{u}_1) \neq f(\boldsymbol{u}_2)$ and $T \geq 2t+1$ we can therefore assume w.l.o.g. that $f(\boldsymbol{u}_1) = m-1$ and $f(\boldsymbol{u}_2) = m$ for some $m \in \mathbb{N}$.

We will prove the lemma for $T = 2t+1$ first. In this case, the parity vectors $\boldsymbol{p}_i$ in the two function regions are illustrated in Table II. Let $\mathrm{wt}(\boldsymbol{u}_1) = (m-1)T + w_1$ and $\mathrm{wt}(\boldsymbol{u}_2) = mT + w_2$ with $w_1, w_2 \in \{0, 1, \ldots, T-1\}$. The corresponding parity vectors are $\boldsymbol{p}(\boldsymbol{u}_1) = \boldsymbol{p}_{w_1+1} = (1^{w_1}0^{2t-w_1})$ and $\boldsymbol{p}(\boldsymbol{u}_2) = \boldsymbol{p}_{w_2+1} = (1^{w_2}0^{2t-w_2})$. Using $d(\boldsymbol{p}_{w_1+1}, \boldsymbol{p}_{w_2+1}) = |w_1 - w_2|$, it follows that $d(\mathsf{Enc}_{\Delta_T}(\boldsymbol{u}_1), \mathsf{Enc}_{\Delta_T}(\boldsymbol{u}_2)) = d(\boldsymbol{u}_1, \boldsymbol{u}_2) + d(\boldsymbol{p}_{w_1+1}, \boldsymbol{p}_{w_2+1}) \geq \mathrm{wt}(\boldsymbol{u}_2) - \mathrm{wt}(\boldsymbol{u}_1) + |w_1 - w_2| = T - w_1 + w_2 + |w_1 - w_2| \geq T = 2t+1$. The case $T > 2t+1$ is proven similarly using that

$$d(\boldsymbol{p}_{w_1+1}, \boldsymbol{p}_{w_2+1}) = \begin{cases} |w_1 - w_2|, & \text{if } w_1 \leq 2t \wedge w_2 \leq 2t, \\ [2t - w_2]^+, & \text{if } w_1 > 2t, \\ [2t - w_1]^+, & \text{if } w_2 > 2t. \end{cases}$$

□

VI. MIN-MAX FUNCTIONS

Assume now that $k = w\ell$ for some integers w and ℓ. In this section, we consider $\boldsymbol{u}$ to be formed of w parts, such that

$\boldsymbol{u} = (\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(w)})$, where each $\boldsymbol{u}^{(i)} \in \mathbb{Z}_2^{\ell}$ is of length ℓ. The function of interest is the min-max function defined next.

Definition 11: The min-max function is defined by

$$\mathrm{mm}_w(\boldsymbol{u}) = (\arg\min_{1\le i\le w} \boldsymbol{u}^{(i)}, \arg\max_{1\le i\le w} \boldsymbol{u}^{(i)}),$$

where $\boldsymbol{u} = (\boldsymbol{u}^{(1)}, \ldots, \boldsymbol{u}^{(w)})$, $\boldsymbol{u}^{(i)} \in \mathbb{Z}_2^{\ell}$ with $k = w\ell$ and the ordering $<$ between the $\boldsymbol{u}^{(i)}$'s is primarily lexicographical (the left-most bit is the most significant) and secondarily, if $\boldsymbol{u}^{(i)} = \boldsymbol{u}^{(j)}$, according to ascending indices.

For example, $\boldsymbol{u} = (\boldsymbol{u}^{(1)}, \boldsymbol{u}^{(2)}, \boldsymbol{u}^{(3)}) = (100, 010, 010)$, has the ordering $\boldsymbol{u}^{(2)} < \boldsymbol{u}^{(3)} < \boldsymbol{u}^{(1)}$ and thus $\mathrm{mm}_w(\boldsymbol{u}) = (2, 1)$. For $w = 1$, the function is constant and for $w = 2$, the function is a binary function and we have an optimal solution from Lemma 5. For $w \ge 3$, we provide two lower bounds on the redundancy in Lemma 9 and Corollary 4. We characterize the function distance matrix of the min-max function in Claims 1 and 2 and obtain an upper bound on the redundancy based on Theorem 2, which is derived in Lemma 10. Since Lemma 10 is obtained using a Gilbert-Varshmov argument, the result is of existential nature. We construct explicit FCCs based on standard error-correcting codes in Construction 3 and Construction 4. Throughout this section we refer to the function distance matrix $\boldsymbol{D}_{\mathrm{mm}}(t, f_1, \ldots, f_E)$ as $\boldsymbol{D}_{\mathrm{mm}}$ for ease of notation. The following example illustrates our results.

Example 3: Consider a min-max function with $w = 3$ and $\ell \ge 3$. From Claim 1 and Claim 2 we obtain the function distance matrix $\boldsymbol{D}_{\mathrm{mm}}$ for this case and any t as follows

$$\boldsymbol{D}_{\mathrm{mm}} = \begin{array}{c|cccccc} \mathrm{f}(\boldsymbol{u}) & (1,2) & (1,3) & (2,1) & (2,3) & (3,1) & (3,2) \\ \hline (1,2) & 0 & 2t & 2t-1 & 2t & 2t & 2t \\ (1,3) & 2t & 0 & 2t & 2t & 2t-1 & 2t \\ (2,1) & 2t-1 & 2t & 0 & 2t & 2t & 2t \\ (2,3) & 2t & 2t & 2t & 0 & 2t & 2t-1 \\ (3,1) & 2t & 2t-1 & 2t & 2t & 0 & 2t \\ (3,2) & 2t & 2t & 2t & 2t-1 & 2t & 0 \end{array}.$$

For example, the function distance between the function values $(1, 2)$ and $(1, 3)$ is 1 since there exist information words $\boldsymbol{u}_1 = (000, 010, 001)$ and $\boldsymbol{u}_2 = (000, 010, 011)$ such that $d(\boldsymbol{u}_1, \boldsymbol{u}_2) = 1$ and $\mathrm{mm}_w(\boldsymbol{u}_1) = (1, 2)$ and $\mathrm{mm}_w(\boldsymbol{u}_2) = (1, 3)$. For $w = 3$ this holds for all pairs of function values except for those of the form (i, j) and (j, i) where at least two bits must be changed to move from one function value to another, i.e., for every $\boldsymbol{u}_1, \boldsymbol{u}_2$ such that $\mathrm{mm}_w(\boldsymbol{u}_1) = (i, j)$ and $\mathrm{mm}_w(\boldsymbol{u}_2) = (j, i)$, we have $d(\boldsymbol{u}_1, \boldsymbol{u}_2) \ge 2$, cf. proof of Claim 2. A possible construction for an FCC is to use a code with cardinality $w(w-1) = 6$ and distance matrix $\boldsymbol{D}_{\mathrm{mm}}$ in the fashion of Theorem 2, i.e., the redundancy vectors are encoded based on $f(\boldsymbol{u})$ instead of $\boldsymbol{u}$. Note that we will observe later that such an encoding yields a redundancy that is not too far from optimality. From Lemma 9, which is presented in the sequel, for $w = 3$ the optimal FCC redundancy is at least $10t/3 - 11/6$. On the other hand, using single-parity check codes, we will construct next an FCC for $w = 3$ with redundancy $r_{\mathrm{SP}} = 4t$ in Construction 3.

We now formally present our results. We start with the lower bound on the redundancy.

Lemma 9: For $w \ge 3$ and $\ell \ge 2$, the optimal redundancy $r_{\mathrm{mm}_w}(k, t)$ is bounded from below by

$$r_{\mathrm{mm}_w}(k, t) \ge \frac{4t(w^2 - w - 1) - 3w^2 + 7w - 5}{(w-1)w}.$$

Proof: Let $\boldsymbol{u}_{i,j} \in \mathbb{Z}_2^k$ with $i, j \in [w]$, $i \ne j$ be $w(w-1)$ information vectors that will be specified later and $\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})$ be their distance matrix. We use the result of Corollary 1 and Lemma 1 to obtain

$$\begin{aligned} r_{\mathrm{mm}_w}(k, t) &\ge N(\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})) \\ &\ge \frac{4}{(w(w-1))^2} \sum_{i,j:i<j} [\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})]_{ij}. \end{aligned}$$

We first prove the lower bound for $\ell = 2$. To obtain a good lower bound, we need to find a suitable set of $w(w-1)$ representative information vectors and characterize their distance matrix $\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})$. We choose the representative information vectors $\boldsymbol{u}_{i,j}$ to be

$$\boldsymbol{u}_{i,j} = (01, \ldots, 01, \underbrace{00}_{\boldsymbol{u}^{(i)}}, \underbrace{11}_{\boldsymbol{u}^{(j)}}, 01, \ldots, 01),$$

where $i, j \in [w]$ and $i \ne j$. Note that $\mathrm{mm}_w(\boldsymbol{u}_{i,j}) = (i, j)$ and therefore the corresponding function values are all distinct. Let further $i', j' \in [w]$ with $i \ne i'$ and $j \ne j'$. We directly see that $d(\boldsymbol{u}_{i,j}, \boldsymbol{u}_{i,j'}) = d(\boldsymbol{u}_{i,j}, \boldsymbol{u}_{i',j}) = 2$ for function values which agree either in the minimum or maximum value. Further, $d(\boldsymbol{u}_{i,j}, \boldsymbol{u}_{i',j'}) = 4$ for function values that agree neither on the minimum nor maximum. For a given $\boldsymbol{u}_{i,j}$, there are thus

- $(w-2)$ information vectors $\boldsymbol{u}_{i,j'}$ at distance 2,
- $(w-2)$ information vectors $\boldsymbol{u}_{i',j}$ at distance 2,
- $(w-1)(w-2)+1$ information vectors $\boldsymbol{u}_{i',j'}$ at distance 4.

Therefore, each row of $\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})$ has $2(w-2)$ entries that are equal to $2t-1$ and $(w-1)(w-2)+1$ entries that are equal to $2t-3$. Having characterized the values of the entries of the distance matrix, we can now write

$$\begin{aligned} r_{\mathrm{mm}_w}(k, t) &\ge \frac{4}{(w(w-1))^2} \sum_{i,j:i<j} [\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})]_{ij} \\ &\overset{(a)}{=} \frac{2}{(w(w-1))^2} \sum_{i,j} [\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})]_{ij} \\ &\overset{(b)}{=} \frac{4t(w^2 - w - 1) - 3w^2 + 7w - 5}{(w-1)w}. \end{aligned}$$

Equation (a) follows from the symmetry of the matrix $\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})$ and equality (b) follows by replacing the values discussed above and rearranging the terms. This proves the lower bound of Lemma 9. The proof for all $\ell > 2$ follows the same steps after setting the $\ell - 2$ left-most bits in every part of each $\boldsymbol{u}_{i,j}$ to 0. □

While this bound provides a good bound for large t and moderate w, we can derive a stronger bound for fixed t and large w as follows.

Corollary 4: For $w \ge 3$ and $\ell \ge 2$, the optimal redundancy $r_{\mathrm{mm}_w}(k, t)$ is bounded from below by

$$r_{\mathrm{mm}_w}(k, t) \ge \log(w(w-1)) + (t-2)\log\log(w(w-1)) - t\log t.$$

Proof: From the proof of Lemma 9, we know that $r_{\mathrm{mm}_w}(k,t) \geq N(\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w}))$. This quantity however can be bounded from below by noting that $d(\boldsymbol{u}_{i,j}, \boldsymbol{u}_{i',j'}) \leq 4$ for any i, j, i', j' (as shown in the same proof) and thus $N(\boldsymbol{D}_{\mathrm{mm}}(t, \boldsymbol{u}_{1,2}, \ldots, \boldsymbol{u}_{w-1,w})) \geq N(w(w-1), 2t-3)$. In other words, the $w(w-1)$ vectors must form a code of minimum distance $2t-3$. Abbreviating $r \triangleq N(w(w-1), 2t-3)$ it follows from a sphere packing argument that $2^r \geq w(w-1)V(r, t-2)$, where $V(r,t) = \sum_{i=0}^{t}\binom{r}{i}$ is the size of the radius-t Hamming sphere over vectors of length r. Consequently,

$$\begin{aligned} r &\geq \log w(w-1) + \log V(r, t-2) \\ &\geq \log w(w-1) + (t-2)\log(r/(t-2)) \\ &\overset{(a)}{\geq} \log w(w-1) + (t-2)\log\log w(w-1) - (t-2)\log t, \end{aligned}$$

where in (a), we used the inequality $r \geq \log w(w-1)$. □

We provide two upper bounds on the optimal redundancy $r_{\mathrm{mm}_w}(k,t)$ of FCCs designed for the min-max function. The first bound (Corollary 5) follows from Lemma 4 and uses standard error-correcting codes. On the other hand, the second bound (Lemma 10) is obtained by examining the function distance matrix of the min-max function and using irregular-distance error-correcting codes.

Corollary 5 (Corollary of Lemma 4): Given t and w such that $t \geq 5$ and $w(w-1) \leq 4t^2$, the optimal redundancy $r_{\mathrm{mm}_w}(k,t)$ is bounded from above by

$$r_{\mathrm{mm}_w}(k,t) \leq \frac{4t}{1 - 2\sqrt{\ln(2t)/2t}}.$$

Proof: Encoding the parity vectors with an error-correcting code of minimum distance $2t$ results in an FCC. The redundancy of this FCC is then equal to the length of the used code. Therefore, the bound holds from Lemma 4. □

Lemma 10: For $w \geq 3$ and $\ell \geq 3$, the optimal redundancy $r_{\mathrm{mm}_w}(k,t)$ of FCCs is bounded from above by

$$r_{\mathrm{mm}_w}(k,t) \leq \min_{r\in\mathbb{N}} \left\{r : \Phi(r) > 0\right\},$$

where $\Phi(r) \triangleq 2^r - (w^2-w-1)V(r, 2t-2) + (4w-8)\binom{r}{2t-1}$.

Proof:

We start by bounding the distance between any two function values.

Claim 1: Consider a min-max function as defined in Definition 11. For all $w \geq 3$ and $\ell \geq 3$ the minimum distance between any two function values (cf. Definition 6) f_1 and f_2 is at most 2, i.e.,

$$\forall f_1, f_2 \in \mathrm{Im}(\mathrm{mm}_w), \quad d_{\mathrm{mm}_w}(f_1, f_2) \leq 2.$$

To prove Claim 1 we need to show that for every two function values $f_1 \neq f_2$, there exist two information vectors $\boldsymbol{u}_1 \neq \boldsymbol{u}_2$ such that $\mathrm{mm}_w(\boldsymbol{u}_1) = f_1$, $\mathrm{mm}_w(\boldsymbol{u}_2) = f_2$ and $d(\boldsymbol{u}_1, \boldsymbol{u}_2) = 2$. We show the existence of such information vectors in Appendix C. Given the result of Claim 1, we know that the entries of $\boldsymbol{D}_{\mathrm{mm}}$, $[\boldsymbol{D}_{\mathrm{mm}}]_{ij} = 2t + 1 - d_{\mathrm{mm}_w}(f_i, f_j)$, are bounded from below by $2t-1$. The remaining part is to count the number of entries that satisfy $[\boldsymbol{D}_{\mathrm{mm}}]_{ij} = 2t$, i.e., the number of values i, j for which $d_{\mathrm{mm}_w}(f_i, f_j) = 1$. We show that the number of such entries is equal to $4w(w-1)(w-2) + 2(w-1)$ by counting the number of function values that satisfy $d_{\mathrm{mm}_w}(f_i, f_j) = 1$.

Claim 2: Consider a min-max function as defined in Definition 11. For all $w \geq 3$ and $\ell \geq 3$, given a function value $f_1 = (i,j)$, the number of function values $f_2 \neq (i,j)$ that satisfy $d_{\mathrm{mm}_w}(f_1, f_2) = 1$ is $4(w-2)$. Therefore, the number of entries in $\boldsymbol{D}_{\mathrm{mm}}$ that is equal to $2t$ is equal to $4w(w-1)(w-2)$.

The proof of Claim 2 consists of finding for every function value f_1 the number of distinct function values f_2 that can be obtained by changing one bit in any information vector $\boldsymbol{u}$ satisfying $\mathrm{mm}_w(\boldsymbol{u}) = f_1$. A formal proof is provided in Appendix D. The results of Claim 1 and Claim 2 characterize the entries of the function distance matrix $\boldsymbol{D}_{\mathrm{mm}}$. Recall that Theorem 2 implies that

$$r_{\mathrm{mm}_w}(k,t) \leq N\left(\boldsymbol{D}_{\mathrm{mm}}\right).$$

We use Lemma 2 and the results of Claim 1 and Claim 2 to prove Lemma 10. From Lemma 2 and by symmetry of $\boldsymbol{D}_{\mathrm{mm}}$ we have

$$N\left(\boldsymbol{D}_{\mathrm{mm}}\right) \leq \min_{r\in\mathbb{N}} \text{ s.t. } \Phi(r) \geq 0,$$

where

$$\Phi'(r) = 2^r - \max_{i\in[w(w-1)]} \sum_{j=1}^{i-1} V\left(r, [\boldsymbol{D}_{\mathrm{mm}}]_{\pi(i)\pi(j)} - 1\right)$$

and π is a permutation of the integers in $[w(w-1)]$. Note that $\sum_{j=1}^{i-1} V(r, [\boldsymbol{D}_{\mathrm{mm}}]_{\pi(i)\pi(j)} - 1)$ is summing all the entries of a given row $\pi(i)$ of $\boldsymbol{D}_{\mathrm{mm}}$. Thus the maximum of this sum can be bounded from above by setting $i = w(w-1)$ and choosing a row with the largest entries.

From Claim 1 and Claim 2, we know that a row i with maximum entries contains exactly one entry equal to 0, $4w-8$ entries equal to $2t$ and the rest is equal to $2t-1$. Given this observation, we obtain that $\Phi(r)$ in the Lemma statement is a lower bound to $\Phi'(r)$ and the lemma follows. □

We give an FCC based on the single-parity check code in Construction 3.

Construction 3: Let $\mathcal{C}_{\mathrm{SP}}$ be a subcode of the single-parity check code of size $w(w-1)$. Replicate every bit in the codewords of $\mathcal{C}_{\mathrm{SP}}$ to t bits. Assign a unique codeword of the expanded version of $\mathcal{C}_{\mathrm{SP}}$ to a redundancy vector $\boldsymbol{p}_{i,j}$ used for all information vectors $\boldsymbol{u}$ such that $f(\boldsymbol{u}) = (i,j)$.

Lemma 11: Construction 3 is an FCC for the min-max function and has redundancy $r_{\mathrm{SP}} = t(\lceil \log(w(w-1)) \rceil + 1)$.

Proof: The lemma follows from the following observations: 1) The length of each codeword in $\mathcal{C}_{\mathrm{SP}}$ is $\lceil \log(w(w-1)) \rceil + 1$; 2) the minimum distance of $\mathcal{C}_{\mathrm{SP}}$ is 2; and 3) replicating every bit in the codewords of $\mathcal{C}_{\mathrm{SP}}$ gives the desired code of length $t(\lceil \log(w(w-1)) \rceil + 1)$, cardinality $w(w-1)$ and minimum distance $2t$. □

We present another FCC based on Reed-Muller codes in Construction 4. For more information about Reed-Muller codes, we refer the reader to [29].

Construction 4: Consider the $\mathrm{RM}(r,m)$ Reed-Muller code of length 2^m, cardinality $k_{\text{r,m}} \triangleq \sum_{i=0}^{r}\binom{m}{i}$, and minimum distance 2^{m-r}. For given w, t choose m such that it is the smallest integer possible for which there exists an integer r satisfying $2^{m-r} \geq 2t$ and $k_{\text{r,m}} \geq \log(w(w-1))$. Denote by $\boldsymbol{p}_{1,2}, \boldsymbol{p}_{1,3}, \ldots, \boldsymbol{p}_{w-1,w}$ an arbitrary subcode of size $w(w-1)$ of the $\mathrm{RM}(r,m)$ code. We then define

$$\mathsf{Enc}_{\mathrm{mm}_w}(\boldsymbol{u}) = (\boldsymbol{u}, \boldsymbol{p}_{\mathrm{mm}_w(\boldsymbol{u})}).$$

Following the arguments of Lemma 11, it is clear that Construction 4 gives an FCC for the min-max function with redundancy $r_{\mathrm{RM}} = 2^m$. To see the importance of this construction, consider the example where t is a power of 2 and $w \leq \sqrt{8t}$. Then, one can use an $\mathrm{RM}(1, \log(4t))$ to obtain an FCC for the min-max function with redundancy equal to $4t$ which is asymptotically, for large w, only 3 bits away from the lower bound of Lemma 9.

VII. Real-Valued Functions

In this section we apply our theoretical results on FCCs to a collection of real-valued functions that take a real number as input and output a real number, i.e., functions of the form $g : \mathbb{R} \to \mathbb{R}$. Throughout this work, however, we consider digital functions that take binary vectors as input and have an arbitrary output, i.e., we consider functions of the form $f : \mathbb{Z}_2^k \to \mathsf{Im}(f)$. To this end, let $\mathrm{b2r} : \mathbb{Z}_2^k \to \mathbb{R}$ be a mapping from the binary information vectors to real numbers. Thus, throughout this section considered functions are[3]

$$\mathrm{RV}_g(\boldsymbol{u}) = g(\mathrm{b2r}(\boldsymbol{u})),$$

where g is one of the functions presented below. While our ideas apply to several binary representations, we opt to explain the results using a fixed precision quantization b2r as follows. Given a fixed precision $\epsilon > 0$, the mapping b2r maps the binary vectors to intervals of size ϵ, i.e.,

$$\mathrm{b2r}(\boldsymbol{u}) = \epsilon\left(\mathrm{bin2dec}(\boldsymbol{u}) - 2^{k-1} + 0.5\right),$$

where $\mathrm{bin2dec} : \mathbb{Z}_2^k \to \{0, 1, \ldots 2^k - 1\}$ is the standard mapping from binary to decimal. Notice that this way, real values in the range of $\pm(2^{k-1} - 0.5)\epsilon$ can be represented, which will be called *quantization intervals* hereafter.

The functions we consider are shown in Fig. 5 and are defined as follows:

- Sigmoid or logistic function: $\sigma(x) = \frac{1}{1+e^{-x}}$ and its derivative $\frac{\partial\sigma(x)}{\partial x} = \frac{e^x}{(1+e^x)^2}$.
- Rectified linear unit (ReLU) function: $\mathrm{ReLU}(x) = \max\{0, x\}$ and its derivative $\frac{\partial \mathrm{ReLU}(x)}{\partial x} = 0$, if $x < 0$ and 1, if $x > 0$.
- Hyperbolic tangent function: $\tanh(x) = \frac{e^x - e^{-x}}{e^x + e^{-x}}$ and its derivative $\frac{\partial \tanh(x)}{\partial x} = 1 - \tanh(x)^2$.

Those functions have practical importance as they are activation functions, and their derivatives, used in neural networks[4].

Throughout this section we discuss FCCs whose encoding is based on the function value only, as in Theorem 2. Thus, the defining quantity of interest is the function distance matrix $\boldsymbol{D}_{\mathrm{RV}_g}(t, f_1, \ldots, f_E)$, which we abbreviate by $\boldsymbol{D}_g$.

We now study the three functions mentioned above. We delay the study of the derivatives of the sigmoid and $\tanh(x)$ function for only after Lemma 13. These three functions can be divided into two classes: a class of functions that are bijective on a certain interval and constant (output equal to 0) otherwise, such as the ReLU function; and a class of functions that are bijective on a certain interval and have approximately constant output for small and large values of x, such as the sigmoid and tanh functions. To see this division notice that numerically one can consider $\tanh(x) = 1$ for all $x \geq 6$ and $\tanh(x) = -1$ for all $x \leq -6$. Similarly $\sigma(x) = 1$ for $x \geq 10$ and $\sigma(x) = 0$ for $x \leq -10$. The ReLU function is a bijective function for all $x > 0$ and is 0 otherwise (cf. Fig. 5).

Let $[a, b] \subset \mathbb{R}$ be the interval in which the function g is bijective and assume for simplicity that ϵ divides $b - a$. For notational convenience, we denote the binary vector representing a certain quantization center c by $\mathbf{w}_i$, $\mathbf{u}_i$ or $\mathbf{v}_i$ if $c < a$, $a \leq c \leq b$ or $c > b$, respectively. In addition we define $d(\boldsymbol{u}_i, \mathbf{v}) \triangleq \min_{\ell} d(\boldsymbol{u}_i, \mathbf{v}_\ell)$ to be the Hamming distance between the binary vector $\boldsymbol{u}_i$ representing a quantization center $c_1 \in [a, b]$ and all binary vectors representing a quantization center $c_2 < a$. We define $d(\boldsymbol{u}_i, \mathbf{v})$ and $d(\mathbf{v}, \mathbf{w})$ similarly.

We characterize the redundancy of an FCC for the considered real-valued functions in Lemma 12 and Lemma 13. Let $g_{00} : \mathbb{R} \to \mathbb{R}$ be a real-valued function that is bijective on an interval $[a, b] \subset \mathbb{R}$ and equal to 0 on $\mathbb{R} \setminus [a, b]$. Fix an $\epsilon > 0$, and define the *symmetric* square matrix $\boldsymbol{D}_{\mathrm{RV00}}$ with $(b - a)/\epsilon + 1$ rows that has for $i \leq j$ the entries

$$[\boldsymbol{D}_{\mathrm{RV00}}]_{ij} = \begin{cases} 0, & \text{if } i = j, \\ 2t{+}1{-}d(\boldsymbol{u}_i, \boldsymbol{u}_j), & \text{if } j \leq \frac{b-a}{\epsilon}, \\ 2t{+}1{-}\min\{d(\boldsymbol{u}_i, \mathbf{v}), d(\boldsymbol{u}_i, \mathbf{w})\}, & \text{otherwise.} \end{cases}$$

Lemma 12: The redundancy of an FCC for the function $\mathrm{RV}_{g_{00}}$ is bounded from above by

$$r_{g_{00}}(k, t) \leq N\left(\boldsymbol{D}_{\mathrm{RV00}}\right).$$

If only one input vector evaluates to 0, the upper bound becomes the optimal redundancy of an FCC for this function. The same holds if several input vectors evaluate to 0 and have similar distance profiles to each of the $\boldsymbol{u}_i$'s. This observation holds for the next lemma as well.

Proof: The proof follows from Theorem 2 by designing the parities based on the function values. On a high level, since all input values in $\mathbb{R} \setminus [a, b]$ have the same output value, then

[3] From a practical point of view, we assume that the data is stored in binary vectors with a predetermined representation and a desired precision. However, during computations, the input is transformed to a real number and the function is computed over the reals with different representation and different precision.

[4] In neural networks, the considered functions are multivariate, they take as input a model vector $\mathbf{a}$ and a weight vector $\mathbf{w}$. However, they only operate on the inner product $\mathbf{w}^T\mathbf{a}$. To that end, we express the inner product of those vectors by the scalar $x = \mathbf{w}^T\mathbf{a}$ and treat those functions as univariate.

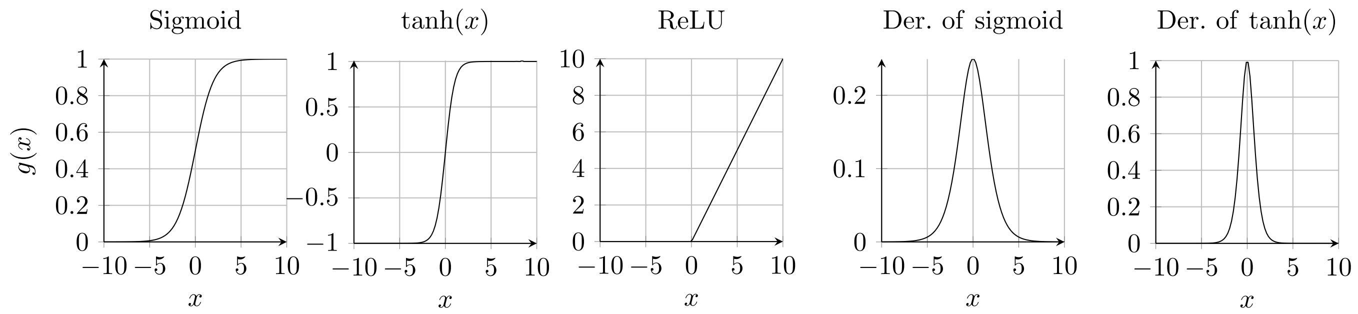


Fig. 5. Plots of the considered real-valued functions. From left to right we plot the sigmoid function, hyperbolic tangent function, the ReLU, the derivative of the sigmoid function and the derivative of the hyperbolic tangent. Observe that the first three functions are bijective on a certain interval of numbers and are approximately constant on one or two intervals. The last two functions are symmetric around 0. For all $x \geq 0$, the last two functions are bijective on a certain interval and 0 otherwise.

the codewords of the form $(\mathbf{w}_i, \boldsymbol{p})$ and $(\mathbf{v}_j, \boldsymbol{p})$ are allowed to be confusable after t errors and can thus have a distance less than $2t+1$. However, the codewords of the form $(\boldsymbol{u}_i, \boldsymbol{p})$ cannot be confusable with any other codeword after t errors. Therefore, for every $\boldsymbol{u}_i$ we search for the closest (in Hamming distance) $\mathbf{v}$ or $\mathbf{w}$ and design the parity vector of the $\mathbf{v}_j$'s and $\mathbf{w}_j$'s accordingly. The same is done for $\boldsymbol{u}_i$ and $\boldsymbol{u}_j$ for $i \neq j$.

Formally, let $\boldsymbol{p}_0, \ldots, \boldsymbol{p}_{\frac{b-a}{\epsilon}}$ be the parity vectors used in the encoding such that $\mathsf{Enc}(\boldsymbol{u}_i) = (\boldsymbol{u}_i, \boldsymbol{p}_i)$ for $i = 1, \ldots, \frac{b-a}{\epsilon}$, $\mathsf{Enc}(\mathbf{w}) = (\mathbf{w}, \boldsymbol{p}_0)$ and $\mathsf{Enc}(\mathbf{v}) = (\mathbf{v}, \boldsymbol{p}_0)$. It follows from Theorem 2 that $r_{g_{00}}(k,t) \leq N\left(\boldsymbol{D}_{\mathrm{RV00}}\right)$. □

Let $g_{01} : \mathbb{R} \to \mathbb{R}$ be a real-valued function that is bijective on an interval $[a,b] \subset \mathbb{R}$ and satisfies $g_{01}(x) = 0$ for all $x < a$ and $g_{01}(x) = 1$ for all $x > b$. Fix a precision ϵ and, for ease of notation, define $\mathbf{v} \triangleq \boldsymbol{u}_{\frac{b-a}{\epsilon}+1}$ and $\mathbf{w} \triangleq \boldsymbol{u}_{\frac{b-a}{\epsilon}+2}$. Let the symmetric matrix $\boldsymbol{D}_{\mathrm{RV01}}$ with $(b-a)/\epsilon + 2$ rows be defined as follows

$$[\boldsymbol{D}_{\mathrm{RV01}}]_{ij} = \begin{cases} 0, & \text{if } i = j, \\ 2t+1-d(\boldsymbol{u}_i, \boldsymbol{u}_j), & \text{otherwise.} \end{cases}$$

Lemma 13: The redundancy of an FCC for the function $\mathrm{RV}_{g_{01}}(\boldsymbol{u}) = g_{01}(\mathrm{b2r}(\boldsymbol{u}))$ is bounded from above by

$$r_{g_{01}}(k,t) \leq N\left(\boldsymbol{D}_{\mathrm{RV01}}\right).$$

The proof is omitted as it follows the same steps of the proof of Lemma 12 while taking care of not confusing any of the $\mathbf{v}_i$'s with any of the $\mathbf{w}_i$'s.

Now we study the derivative of $\sigma(x)$ and $\tanh(x)$. Both functions are symmetric around 0 and are bijective on an interval $[0,a]$ and constant otherwise. Numerically, one could consider the derivative of $\sigma(x)$ to be equal to 0 outside the interval $[-10,10]$ and the derivative of $\tanh(x)$ to be 0 outside the interval $[-6,6]$.

For this set of functions we abuse notation and denote by $\boldsymbol{u}_i$ the binary representation of a quantization center $c \in [0,a]$ and by $-\boldsymbol{u}_i$ the binary representation of the quantization center $-c$. Similarly $\mathbf{v}_i$ is the binary representation of $c > a$ and $-\mathbf{v}_i$ is the binary representation of $-c < -a$. We define $d(\pm\boldsymbol{u}_i, \pm\boldsymbol{u}_j) \triangleq \min\{d(\boldsymbol{u}_i,\boldsymbol{u}_j), d(\boldsymbol{u}_i,-\boldsymbol{u}_j), d(-\boldsymbol{u}_i,\boldsymbol{u}_j), d(-\boldsymbol{u}_i,-\boldsymbol{u}_j)\}$ and define $d(\pm\boldsymbol{u}_i, \pm\mathbf{v})$ similarly. This notation makes the following definitions easier to present.

Let $g_{\mathrm{sym}} : \mathbb{R} \to \mathbb{R}$ be a real-valued function with $g(x) = g(-x)$, bijective on an interval $[0,a] \subset \mathbb{R}$ and is constant for $x > a$. Fix a precision ϵ and define the *symmetric* square matrix $\boldsymbol{D}_{\mathrm{RV-sym}}$ with $\frac{a}{\epsilon}+1$ rows that has for $i \leq j$ the entries

$$[\boldsymbol{D}_{\mathrm{RV-sym}}]_{ij} = \begin{cases} 0, & \text{if } i = j, \\ 2t+1-d(\pm\boldsymbol{u}_i, \pm\boldsymbol{u}_j), & \text{if } j \leq \frac{a}{\epsilon}, \\ 2t+1-d(\pm\boldsymbol{u}_i, \pm\mathbf{v}), & \text{otherwise.} \end{cases}$$

Lemma 14: The redundancy of an FCC for the function $\mathrm{RV}_{g_{\mathrm{sym}}}(\boldsymbol{u}) = g_{\mathrm{sym}}(\mathrm{b2r}(\boldsymbol{u}))$ is then bounded from above by

$$r_{g_{\mathrm{sym}}} \leq N\left(\boldsymbol{D}_{\mathrm{RV-sym}}\right).$$

The proof is omitted as it follows the same steps of the proof of Lemma 12.

VIII. Conclusion

We introduced a new class of codes called function-correcting codes which encode a message to allow a successful recovery of a certain attribute or a function value of this message after transmission over an erroneous channel. This encoding potentially reduces the redundancy compared to error-correcting codes by leveraging the side information given to the receiver by the knowledge of the possibly erroneous original message and the desired function.

We considered an encoding setup in which the message itself is also transmitted and restricted our attention to substitution channels with at most t errors. For this setting, we derived lower and upper bounds on the redundancy of FCCs by establishing a connection to irregular-distance codes. Further, we examined several functions of interest for which we derived explicit distance matrices, such that an irregular-distance code satisfying the distance matrix gives an optimal FCC for the function at hand. Furthermore, we derived lower bounds and constructed FCCs for each specific function. Our constructions have optimal redundancy for the Hamming weight distribution functions. For the min-max function, we construct almost optimal codes. For the Hamming weight function there is still a gap of roughly $\frac{2}{3}t$ between the lower bound and the provided construction, leaving the problem of finding optimal FCCs open. For real-valued functions, a rigorous study of the distance profile of the input vectors is needed to understand the gap between the achievable redundancy and the lower bound. Further research directions on this topic include the study of FCCs for other functions of interest and under different channels.

Appendix A
Derivations of Redundancies in Table I

We start by deriving the redundancy obtained by employing a standard error-correcting onto the data, labeled as the column "*ECC on Data*" in Table I. This means, the data vector $\boldsymbol{u}$ is encoded with a systematic code of dimension k and minimum distance $2t+1$. The redundancy part $\boldsymbol{p}$ of this systematic code is then appended to $\boldsymbol{u}$, resulting in $(\boldsymbol{u}, \boldsymbol{p})$. Clearly, with such a construction it is possible to reconstruct $\boldsymbol{u}$ at the receiver and thus $f(\boldsymbol{u})$. It is known [29, Ch.5.5] that there exists a binary alternant code of length n, minimum distance $2t+1$ and redundancy at most $r \leq t\lceil \log n \rceil$. Since $n = k + r$,

$$\begin{aligned} r &\leq t\lceil \log(k+r) \rceil \leq t\log(k+r) + t \\ &= t\log k + t\log(1 + r/k) + t \\ &\leq t\log k + t\frac{r\log \mathrm{e}}{k} + t. \end{aligned}$$

It follows that

$$r \leq \frac{t\log k + t}{(1 - t/k\log \mathrm{e})}$$

and thus, for large k and fixed t, the dominant term is $t\log k$.

We now turn to derive the redundancy obtained by a direct approach of encoding the function values, which corresponds to the column "*ECC on Function Values*" in Table I. More precisely, we encode the function value $f(\boldsymbol{u})$ with a (possibly non-systematic) code of cardinality E (recall that E is the size of the image of f) and minimum distance $2t+1$. The resulting *codeword* $\boldsymbol{c}$ is then appended to $\boldsymbol{u}$, resulting in $(\boldsymbol{u}, \boldsymbol{c})$. Also in this case, it is possible to retrieve $f(\boldsymbol{u})$ by decoding the function value from the received word corresponding to $\boldsymbol{c}$ and simply ignoring the information part $\boldsymbol{u}$. In this case, the redundancy of our construction is given by the length of the employed code. Using alternant codes, we obtain for the redundancy of the alternant code

$$\begin{aligned} r_{\text{alt}} &\leq t\lceil \log(\log\lceil |E| \rceil + r_{\text{alt}}) \rceil \\ &\leq t\log\log|E| + t + t(1 + r_{\text{alt}})\log \mathrm{e}/\log|E| \end{aligned}$$

and thus

$$r_{\text{alt}} \leq \frac{t\log\log|E| + t(1 + \log \mathrm{e})}{1 - t/\log|E|\log \mathrm{e}}.$$

Consequently, the redundancy of the direct approach is given by the length of the alternating code $r = \lceil \log|E| \rceil + r_{\text{alt}}$. For sufficiently large $|E|$ and fixed t this is adequately approximated by $\log|E| + t\log\log|E|$.

Appendix B
Proof of Lemma 4

Proof of Lemma 4: Lemma 2 states that there exists a code of cardinality M, minimum distance D and length r, if $2^r > MV(r, D-1)$. For $D-1 \leq r/2$, we can use [28, Lemma4.7.2] to bound the size of the Hamming ball to $V(r, D-1) \leq 2^r \mathrm{e}^{-2r(\frac{1}{2} - \frac{D-1}{r})^2}$. Combining these two results, we obtain that if $2^r > M2^r \mathrm{e}^{-2r(\frac{1}{2} - \frac{D-1}{r})^2}$, then there exists an $[M, D]$ code of length r. Setting $D = r/2 - \epsilon r$ for some $0 < \epsilon \leq \frac{1}{2}$, we can deduce that there exists an $[M, D]$ code of length r satisfying $M \leq \mathrm{e}^{2r\epsilon^2}$. Choosing $\epsilon = \sqrt{\ln(r)/r}$, we obtain that $r = 2D/(1 - 2\sqrt{\ln(r)/r})$. Here we require $r \geq 10$ such that $\epsilon \leq \frac{1}{2}$. We can then use that $\ln(D)/D \geq \ln(r)/r$ for $r \geq D \geq 3$ and we obtain the lemma's statement. □

Appendix C
Proof of Claim 1

Proof of Claim 1: We give a proof for $\ell = 3$. For $\ell > 3$, we can restrict all the bits of all $\boldsymbol{u}^{(v)}$, $v \in [w]$ to be 0 except for the three least significant bits and apply the same proof of $\ell = 3$. We show that for all $i, j, i', j' \in [w]$, $(i, j) \neq (i', j')$ there exist two information words $\boldsymbol{u}, \boldsymbol{u}'$ such that $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$ and $\mathrm{mm}_w(\boldsymbol{u}') = (i', j')$, where $d(\boldsymbol{u}, \boldsymbol{u}') = 2$. We split the proof into the following three cases.

- *$i' \leq i$:* To change $\boldsymbol{u}$ into $\boldsymbol{u}'$ satisfying $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$ and $\mathrm{mm}_w(\boldsymbol{u}') = (i', j')$, consider $\boldsymbol{u}$ to be of the form

  $$\boldsymbol{u} = (001, \ldots, \underbrace{000}_{\boldsymbol{u}^{(i)}}, 001, \ldots, \underbrace{010}_{\boldsymbol{u}^{(j)}}, 001, \ldots, 001).$$

  Note that $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$ by definition of mm_w. We can change $\boldsymbol{u}$ to $\boldsymbol{u}'$ as follows. First, if $i' < i$ flip the third bit of $\boldsymbol{u}^{(i')}$, (so that $\boldsymbol{u}^{(i')} = (000)$) to change the function value to (i', j). To change j to j', it is sufficient to flip the first bit of $\boldsymbol{u}^{(j')}$. Thus, $d_{\mathrm{mm}_w}((i, j), (i', j')) \leq 2$ because we could edit $\boldsymbol{u}$ with $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$ to $\boldsymbol{u}'$ with $\mathrm{mm}_w(\boldsymbol{u}') = (i', j')$ using only two substitutions.
- *$i' > i$, $i' \neq j$:* Consider $\boldsymbol{u}$ to be of the form

  $$\boldsymbol{u} = (001, \ldots, \underbrace{000}_{\boldsymbol{u}^{(i)}}, 001, \ldots, \underbrace{000}_{\boldsymbol{u}^{(i')}}, \underbrace{010}_{\boldsymbol{u}^{(j)}}, 001, \ldots, 001).$$

  Note that $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$ by definition of mm_w. We can change $\boldsymbol{u}$ to $\boldsymbol{u}'$ as follows. First flip the third bit of $\boldsymbol{u}^{(i)}$, (so that $\boldsymbol{u}^{(i)} = (001)$) to change the function value to (i', j). To change j to j', it is sufficient to flip the first bit of $\boldsymbol{u}^{(j')}$.
- *$i' > i$ and $i' = j$:* Consider $\boldsymbol{u}$ to be of the form

  $$\boldsymbol{u} = (010, \ldots, \underbrace{001}_{\boldsymbol{u}^{(i)}}, 010, \ldots, \underbrace{100}_{\boldsymbol{u}^{(j)}}, 010, \ldots, 010). \quad (1)$$

  Note that $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$ by definition of mm_w. We can change $\boldsymbol{u}$ to $\boldsymbol{u}'$ as follows. Flip the first bit of $\boldsymbol{u}^{(j)}$, (so that $\boldsymbol{u}^{(j)} = (000)$) to change the function value to $(j, 1) = (i', 1)$ (or $(j, 2)$, if $j = 1$). To obtain j' as the maximum, it is sufficient to flip the first bit of $\boldsymbol{u}^{(j')}$.

□

Appendix D
Proof of Claim 2

Proof of Claim 2: We give a proof for $\ell = 3$. For $\ell > 3$, we can restrict all the bits of all $\boldsymbol{u}^{(v)}$, $v \in [w]$ to be 0 except for the three least significant bits and apply the same proof of $\ell = 3$. Fix $f_1 \triangleq (i, j)$ and consider all information words $\boldsymbol{u}$ such that $\mathrm{mm}_w(\boldsymbol{u}) = f_1$. Note that for any $\boldsymbol{u}$, the $\boldsymbol{u}^{(v)}$'s form a totally ordered set and therefore can

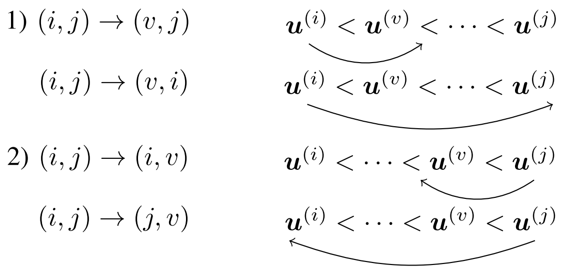

1) $(i,j) \to (v,j)$
$\boldsymbol{u}^{(i)} < \boldsymbol{u}^{(v)} < \cdots < \boldsymbol{u}^{(j)}$
$(i,j) \to (v,i)$
$\boldsymbol{u}^{(i)} < \boldsymbol{u}^{(v)} < \cdots < \boldsymbol{u}^{(j)}$
2) $(i,j) \to (i,v)$
$\boldsymbol{u}^{(i)} < \cdots < \boldsymbol{u}^{(v)} < \boldsymbol{u}^{(j)}$
$(i,j) \to (j,v)$
$\boldsymbol{u}^{(i)} < \cdots < \boldsymbol{u}^{(v)} < \boldsymbol{u}^{(j)}$

Fig. 6. Illustration of the different editing operations in the proof of Claim 2.

be arranged in a chain, as illustrated in Fig. 6. By definition, for any f_2 with $d_{\mathrm{mm}_w}(f_1, f_2) = 1$, there exists a $\boldsymbol{u}$ with $\mathrm{mm}_w(\boldsymbol{u}) = f_1$, such that, by flipping one bit in $\boldsymbol{u}$, the function value changes from f_1 to f_2. We find all possible function values that can be obtained after a single bit flip in some $\boldsymbol{u}$ with $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$. We distinguish between the following types of edit operations.

1) Change one bit in $\boldsymbol{u}^{(i)}$. First, change $\boldsymbol{u}^{(i)}$ such that the result becomes larger then $\boldsymbol{u}^{(i)}$, but smaller than $\boldsymbol{u}^{(j)}$. This way it is only possible to change the function value to (v, j), for an arbitrary $v \in [w] \setminus \{i, j\}$. This can in fact be achieved by choosing $\boldsymbol{u}$ to be

$$\boldsymbol{u} = (011, \ldots, \underbrace{001}_{\boldsymbol{u}^{(i)}}, \underbrace{010}_{\boldsymbol{u}^{(v)}}, 011, \ldots, \underbrace{111}_{\boldsymbol{u}^{(j)}}, 011, \ldots, 011),$$

and flipping the first bit of $\boldsymbol{u}^{(i)}$ (so that $\boldsymbol{u}^{(i)} = (101)$). Note that $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$.

Second, change $\boldsymbol{u}^{(i)}$ such that it becomes larger than $\boldsymbol{u}^{(j)}$. This way, it is only possible to change the function value to (v, i), $v \in [w] \setminus \{i, j\}$. This can be achieved by choosing $\boldsymbol{u}$ to be

$$\boldsymbol{u} = (011, \ldots, \underbrace{001}_{\boldsymbol{u}^{(i)}}, \underbrace{010}_{\boldsymbol{u}^{(v)}}, 011, \ldots, \underbrace{100}_{\boldsymbol{u}^{(j)}}, 011, \ldots, 011)$$

and flipping the first bit of $\boldsymbol{u}^{(i)}$ (so that $\boldsymbol{u}^{(i)} = (101)$). For an illustration, see Fig. 6.

2) Change one bit in $\boldsymbol{u}^{(j)}$. First, we change $\boldsymbol{u}^{(j)}$ such that the result becomes smaller then $\boldsymbol{u}^{(j)}$, but larger than $\boldsymbol{u}^{(i)}$. This way it is only possible to change the function value to (i, v), for an arbitrary $v \in [w] \setminus \{i, j\}$. This can in fact be achieved by choosing $\boldsymbol{u}$ to be

$$\boldsymbol{u} = (100, \ldots, \underbrace{000}_{\boldsymbol{u}^{(i)}}, \underbrace{101}_{\boldsymbol{u}^{(v)}}, 100, \ldots, \underbrace{110}_{\boldsymbol{u}^{(j)}}, 100, \ldots, 100)$$

and flipping the first bit of $\boldsymbol{u}^{(j)}$ (so that $\boldsymbol{u}^{(j)} = (010)$). Note that $\mathrm{mm}_w(\boldsymbol{u}) = (i, j)$.

Second, we change $\boldsymbol{u}^{(j)}$ such that it becomes smaller than $\boldsymbol{u}^{(i)}$. This way, is is only possible to change the function value to (j, v), $v \in [w] \setminus \{i, j\}$. This can be achieved by choosing $\boldsymbol{u}$ to be

$$\boldsymbol{u} = (100, \ldots, \underbrace{011}_{\boldsymbol{u}^{(i)}}, \underbrace{101}_{\boldsymbol{u}^{(v)}}, 100, \ldots, \underbrace{110}_{\boldsymbol{u}^{(j)}}, 100, \ldots, 100)$$

and flipping the first bit of $\boldsymbol{u}^{(j)}$ (so that $\boldsymbol{u}^{(j)} = (010)$).

3) Change one bit in $\boldsymbol{u}^{(v)}$, $v \in [w] \setminus \{i, j\}$. This does not yield any additional function values that can be reached, since it is only possible to obtain (v, j) or (i, v).

Since the resulting function values in cases 1) and 2) are distinct, for each f_1, there exist $4(w-2)$ values f_2 with $f_1 \neq f_2$ and $d_{\mathrm{mm}_w}(f_1, f_2)$. Using further, that there are $w(w-1)$ function values, the total number of entries in $\boldsymbol{D}_{\mathrm{mm}}$ that are equal to $2t$ is equal to $4w(w-1)(w-2)$. □

References

[1] A. Lenz, R. Bitar, A. Wachter-Zeh, and E. Yaakobi, "Function-correcting codes," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Melbourne, VIC, Australia, Jul. 2021, pp. 1290–1295.

[2] B. Masnick and J. Wolf, "On linear unequal error protection codes," *IEEE Trans. Inf. Theory*, vol. IT-13, no. 4, pp. 600–607, Oct. 1967.

[3] I. Boyarinov and G. Katsman, "Linear unequal error protection codes," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 2, pp. 168–175, Mar. 1981.

[4] C. Schoeny, F. Sala, M. Gottscho, I. Alam, P. Gupta, and L. Dolecek, "Context-aware resiliency: Unequal message protection for random-access memories," *IEEE Trans. Inf. Theory*, vol. 65, no. 10, pp. 6146–6159, Oct. 2019.

[5] S. Borade, B. Nakiboglu, and L. Zheng, "Unequal error protection: An information-theoretic perspective," *IEEE Trans. Inf. Theory*, vol. 55, no. 12, pp. 5511–5539, Dec. 2009.

[6] R. Ahlswede and I. Csiszar, "To get a bit of information may be as hard as to get full information," *IEEE Trans. Inf. Theory*, vol. IT-27, no. 4, pp. 398–408, Jul. 1981.

[7] A. Orlitsky and J. R. Roche, "Coding for computing," *IEEE Trans. Inf. Theory*, vol. 47, no. 3, pp. 903–917, Mar. 2001.

[8] S. Kuzuoka and S. Watanabe, "On distributed computing for functions with certain structures," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Cambridge, U.K., Sep. 2016, pp. 6–10.

[9] H. Witsenhausen, "The zero-error side information problem and chromatic numbers (Corresp.)," *IEEE Trans. Inf. Theory*, vol. IT-22, no. 5, pp. 592–593, Sep. 1976.

[10] X. Wang, A. J. Budkuley, A. Bogdanov, and S. Jaggi, "When are large codes possible for AVCs?" in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Paris, France, Jul. 2019, pp. 632–636.

[11] K. Mazooji, F. Sala, G. Van den Broeck, and L. Dolecek, "Robust channel coding strategies for machine learning data," in *Proc. 54th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Monticello, IL, USA, Sep. 2016, pp. 609–616.

[12] S. Kabir, F. Sala, G. Van den Broeck, and L. Dolecek, "Coded machine learning: Joint informed replication and learning for linear regression," in *Proc. 55th Annu. Allerton Conf. Commun., Control, Comput. (Allerton)*, Monticello, IL, USA, Oct. 2017, pp. 1248–1255.

[13] K. Huang, P. H. Siegel, and A. Jiang, "Functional error correction for robust neural networks," *IEEE J. Sel. Areas Inf. Theory*, vol. 1, no. 1, pp. 267–276, May 2020.

[14] N. Raviv, A. Kelley, M. Guo, and Y. Vorobeychik, "Enhancing robustness of neural networks through Fourier stabilization," in *Proc. Int. Conf. Mach. Learn.*, Jul. 2021, p. 10.

[15] R. M. Roth, "Fault-tolerant dot-product engines," *IEEE Trans. Inf. Theory*, vol. 65, no. 4, pp. 2046–2057, Apr. 2019.

[16] R. M. Roth, "Analog error-correcting codes," *IEEE Trans. Inf. Theory*, vol. 66, no. 7, pp. 4075–4088, Jul. 2020.

[17] E. Dupraz and L. R. Varshney, "Noisy in-memory recursive computation with memristor crossbars," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Los Angeles, CA, USA, Jun. 2020, pp. 804–809.

[18] J. H. van Lint, *Introduction to Coding Theory*. Berlin, Germany: Springer, 1999.

[19] J. Gu and T. Fuja, "A generalized Gilbert–Varshamov bound derived via analysis of a code-search algorithm," *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 1089–1093, May 1993.

[20] L. M. G. M. Tolhuizen, "The generalized Gilbert–Varshamov bound is implied by Turan's theorem [code construction]," *IEEE Trans. Inf. Theory*, vol. 43, no. 5, pp. 1605–1606, Sep. 1997.

[21] R. M. Karp, "Reducibility among combinatorial problems," in *Complexity of Computer Computations*, R. E. Miller, J. W. Thatcher, and J. D. Bohlinger, Eds. Cham, Switzerland: Springer, 1972, pp. 85–103.

[22] M. Plotkin, "Binary codes with specified minimum distance," *IEEE Trans. Inf. Theory*, vol. IT-6, no. 4, pp. 445–450, Sep. 1960.

[23] E. N. Gilbert, "A comparison of signalling alphabets," *Bell Syst. Tech. J.*, vol. 31, no. 3, pp. 504–522, May 1952.

[24] R. R. Varshamov, "Estimate of the number of signals in error correcting codes," *Doklady Akademii Nauk SSSR*, vol. 117, no. 5, pp. 739–741, 1957.

[25] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes*, Amsterdam, The Netherlands: Elsevier, 2007.

[26] K. J. Horadam, *Hadamard Matrices and Their Applications*. Princeton, NJ, USA: Princeton Univ. Press, Dec. 2007.

[27] H. Lin, S. M. Moser, and P. Chen, "Weak flip codes and their optimality on the binary erasure channel," *IEEE Trans. Inf. Theory*, vol. 64, no. 7, pp. 5191–5218, Jul. 2018.

[28] R. B. Ash, *Information Theory*. New York, NY, USA: Dover, 1990.

[29] R. Roth, *Introduction to Coding Theory*. Cambridge, U.K.: Cambridge Univ. Press, 2006.

Andreas Lenz (Student Member, IEEE) received the B.Sc. and M.Sc. degrees (Hons.) in electrical engineering and information technology from Technische Université Ménchen (TUM), Germany, and the Ph.D. degree (summa cum laude) in coding for modern memories from TUM in 2022. His research interests include signal processing, coding theory, and information theory.

Rawad Bitar (Member, IEEE) received the Diploma degree in computer and communication engineering from the Faculty of Engineering, Lebanese University, Roumieh, Lebanon, in 2013, the M.S. degree from the Doctoral School, Lebanese University, Tripoli, Lebanon, in 2014, and the Ph.D. degree in electrical engineering from Rutgers University, New Brunswick, NJ, USA, in 2020. He is currently a Post-Doctoral Researcher with the Technical University of Munich, doing a habilitation. His research interests include information theory and coding theory with a focus on coding for insertions and deletions and coding for information theoretically secure distributed systems with application to machine learning.

Antonia Wachter-Zeh (Senior Member, IEEE) received the M.Sc. degree in communications technology from Ulm University, Germany, in 2009, and the dual Ph.D. degree from Ulm University and Universite de Rennes 1, Rennes, France, in 2013. From 2013 to 2016, she was a Post-Doctoral Researcher with the Technion—Israel Institute of Technology, Haifa, Israel. From 2016 to 2020, she was a Tenure Track Assistant Professor with the Technical University of Munich (TUM), Munich, Germany, where she is currently an Associate Professor with the School of Computation, Information and Technology. She was a recipient of the DFG Heinz Maier-Leibnitz-Preis and an ERC Starting Grant. She is currently an Associate Editor of the IEEE TRANSACTIONS ON INFORMATION THEORY. Her research interests include coding theory, cryptography and information theory and their application to storage, communications, privacy, security, and machine learning.

Eitan Yaakobi (Senior Member, IEEE) received the B.A. degree in computer science and mathematics and the M.Sc. degree in computer science from the Technion—Israel Institute of Technology, Haifa, Israel, in 2005 and 2007, respectively, and the Ph.D. degree in electrical engineering from the University of California at San Diego, San Diego, in 2011. From 2011 to 2013, he was a Post-Doctoral Researcher with the Department of Electrical Engineering, California Institute of Technology, and the Center for Memory and Recording Research, University of California at San Diego. He is currently an Associate Professor with the Computer Science Department, Technion—Israel Institute of Technology, where he also holds a courtesy appointment with the Electrical and Computer Engineering (ECE) Department. His research interests include information and coding theory with applications to non-volatile memories, associative memories, DNA storage, data storage and retrieval, and private information retrieval. He received the Marconi Society Young Scholar in 2009 and the Intel Ph.D. Fellowship (2010–2011). Since 2020, he has been serving as an Associate Editor for Coding and Decoding for the IEEE TRANSACTIONS ON INFORMATION THEORY. Since 2016, he has been with the Center for Memory and Recording Research, University of California at San Diego, and since 2018, he has been with the Institute of Advanced Studies, Technical University of Munich, where he holds a four-year Hans Fischer Fellowship, funded by the German Excellence Initiative and the EU Seventh Framework Program. He was a recipient of several grants, including the ERC Consolidator Grant.