Signature Codes for a Noisy Adder Multiple Access Channel
Gökber Erdoğan, Georg Maringer, Nikita Polyanskii

Abstract—In this work, we consider q-ary signature codes of length k and size n for a noisy adder multiple access channel. A signature code in this model has the property that any subset of codewords can be uniquely reconstructed based on any vector that is obtained from the sum (over integers) of these codewords. We show that there exists an algorithm to construct a signature code of length \( k = \frac{2 \log n}{\log(q+\log n)} + \mathcal{O}\left(\frac{n}{\log n}\right) \) capable of correcting \( \tau k \) errors at the channel output, where \( 0 \leq \tau < \frac{1}{2q} \). Furthermore, we present an explicit construction of signature codewords with polynomial complexity being able to correct up to \( (\frac{q-1}{q^2} - \epsilon) k \) errors for a codeword length \( k = \mathcal{O}\left(\frac{n}{\log n}\right) \), where \( \epsilon \) is a small non-negative number. Moreover, we prove several non-existence results (converse bounds) for q-ary signature codes enabling error correction.

I. INTRODUCTION

The problem of determining an n-bit number by asking questions for the sum of a subsequence of its bits has been addressed by scientists from different research backgrounds for over fifty years. In coding theory, the problem corresponds to signature codes for the binary adder multiple access channel (MAC), whereas in combinatorics, it is commonly referred to as the coin weighing problem.

In this paper, we discuss a non-binary generalization of this problem. Consider a set of n users where the i-th user gets assigned a signature codeword \( s_i \in \{0, 1, \ldots, q-1\}^{k\times 1} \) with \( q \geq 2 \). Each user is associated to a channel input \( X_i, \ i \in \{1, 2, \ldots, n\} \). If a user is active, they send their signature codeword \( (X_i = s_i) \); otherwise, they send the all-zero word \( (X_i = \{0\}^{k\times1}) \). The output of the q-ary adder MAC is then defined to be \( Y \triangleq \sum_{i=1}^{n} X_i \), \( Y \in \{0, 1, \ldots, n(q-1)\}^{k\times1} \). The goal is to identify the set of active users by observing the output \( Y \), assuming each user’s signature codeword is given. Thereby, the natural question is how to minimize the length \( k \) of a signature code given its size \( n \).

For \( q = 2 \), an equivalent scenario is the coin weighing problem with non-adaptive weighings. Within this problem setting there are a total of \( n \) coins, some of which are genuine coins with weight \( g \) and the rest are counterfeit coins with weight \( c \), where both \( g \) and \( c \) are known. The goal is to determine the counterfeit coins with as few weighing operations as possible.

A weighing operation determines the weight of an arbitrary subset of the initial \( n \)-coin set. The term non-adaptive refers to the fact that the weighing operations cannot be adapted according to the results of previous weighings.

Representing \( n \) coins, we define \( \vec{u} \in \{0, 1\}^{1\times n} \) as the unknown information sequence. In addition, we define \( M \in \{0, 1\}^{k\times n} \) as a predefined binary query matrix, where each row is a weighing operation, i.e., a query. We finally define the answer sequence \( \vec{w} \in \{0, 1, \ldots, n\}^{k\times1} \) and by definition \( \vec{w} \triangleq \vec{M}\vec{u}^T \).

Referring back to adder MAC, the nonzero positions in \( \vec{u} \) represent the active users, and the zero positions represent the inactive users. So the coin weighing problem translates to active users sending the respective column of the query matrix through the channel, and inactive users sending the all-zero codeword. Also note that \( \vec{w} \) is equivalent to the channel output \( Y \).

In this paper, we will mainly investigate signature codes in a combinatorial error model for a noisy q-ary MAC. This means that if up to \( \tau k \) errors are injected in an adversarial manner into the channel output \( Y \) for \( 0 \leq \tau \leq 1 \), the set of active users shall be uniquely determined.

A. Related Works

The coin weighing problem has been introduced by Shapiro in [1]. Erdős and Rényi in [2] provided the converse bound on the number of weighings. Lindström in [3], and Cantor and Mills in [4] each provided explicit constructions for the coin-weighing problem which are order-optimal as the number of coins \( n \to \infty \). Bshouty in [5] considered the coin weighing problem in the presence of noise.

The problem of constructing binary uniquely decodable signature codes for the adder MAC has been studied by Chang and Weldon in [6], by van der Meulen and Vangheluwe in [7]. Gritsenko et al. in [8] discuss the construction of binary signature codes for the noisy adder MAC when the number of active users is limited by a constant number. Under the guise of detecting sets, non-binary signature codes for the noiseless setting have been studied by Lindström in [3], where he provided an order-optimal code construction of size \( n \) for any fixed alphabet size \( q \geq 2 \) and \( n \to \infty \).
A relevant research direction is devoted to the Mastermind game. In this game, one player conceals a q-ary n-length vector and the second players tries to guess the vector by asking queries. Each query is an n-length vector and the response to the query is the Hamming distance between the vectors. For q = 2, this problem has been shown to be equivalent to the coin weighing problem (up to at most one query) [9]. Chvatá in [10] initiated the study of the q-ary non-adaptive version of the Mastermind game. The follow-up works [11], [12] established the order-optimal strategies for fixed q and n → ∞.

B. Our Contribution

In this paper, we consider q-ary signature codes for the noisy adder MAC. By the double counting argument, we obtain a converse bound for the q-ary case analogously to the binary result presented in [5]. We present a random construction for signature codes as well as two explicit constructions. The term explicit construction refers to the fact that we know how to construct a signature code for the given case in polynomial time. The first explicit construction performs well if the number of errors t is small and has been generated from scratch. It uses signature codes for the noiseless case that have been introduced by Lindström in [3] and combines them with Reed-Solomon codes. The second construction is based on the previously mentioned random construction and is the method of choice for large t, e.g., t = τk for a constant 0 ≤ τ ≤ q−1. More specifically, the explicit construction is obtained by an exhaustive search to find short signature codes and by combining them with good low rate codes via Kronecker products. This enables the design of signature codes that tolerate a designated fraction of errors.

For q = 2, Bshouty presented several results in [5] and some of his approaches inspired the methodology to obtain the probabilistic results for general q presented in this paper. However, the generalization of approaches is not straightforward. In particular, the random construction required us to discover properties of the generalized Pascal’s Triangle.

C. Outline

The remainder of the paper is organized as follows. In Section II, we introduce the notation used throughout the paper alongside generalized Pascal’s triangles. Furthermore, we define signature codes and we present a converse bound discovered by Bshouty in [5]. In Section III, we provide a random construction for a signature code tolerating t < q−1/k errors in the channel output. Furthermore, we show the aforementioned two explicit constructions of signature codes for the q-ary MAC. Moreover, we provide a converse bound for the q-ary case. Section IV concludes the paper.

The proofs for all lemmas and corollaries can be found in the full version of the paper [13]. For theorems, proof sketches are included in this paper.

II. Preliminaries

A. Notation

We denote the set of integers by \( \mathbb{Z} \), the set of positive integers by \( \mathbb{Z}^+ \) and the set of negative integers by \( \mathbb{Z}^- \). Similarly, we denote the set of nonnegative integers by \( \mathbb{Z}_0^+ = \mathbb{Z}^+ \cup \{0\} \). For a positive integer \( b \), \( \mathbb{Z}_0^+(b) \) denotes the set \( \{0, 1, \ldots, b-1\} \). Logarithms are to the base 2 throughout this work and simply denoted by \( \log \), \( H_2(\cdot) \) denotes the binary entropy function. \( wt(y) \) denotes the Hamming weight of the integer sequence \( y \), where the Hamming weight is defined as the number of nonzero positions in a given sequence. \( \otimes \) denotes the Kronecker product of two matrices.

B. Signature Codes

A matrix \( M \in \{0,1,\ldots,q-1\}^{k \times n} \) is called a q-ary signature code capable of correcting \( t \) errors if for any two distinct binary vectors \( \vec{u}_1, \vec{u}_2 \in \{0,1\}^k \times n \) and any integer vectors \( \vec{e}_1, \vec{e}_2 \in \mathbb{Z}^{k \times n} \) with \( wt(\vec{e}_1) \leq t \) and \( wt(\vec{e}_2) \leq t \), the vectors \( M \vec{u}_1 + \vec{e}_1 \) and \( M \vec{u}_2 + \vec{e}_2 \) are different in at least one position.

C. Pascal’s Triangle

Define \( C_{k,n} \) as the coefficient of \( x^k \) in the expression \((1 + x)^n\), where \( k, n \in \mathbb{Z}_0^+ \) and \( 0 \leq k \leq n \). Note that \( C_{k,n} = \binom{n}{k} \) are the binomial coefficients which can also be defined in a recursive way, i.e. \( C_{k,n} = C_{k,n-1} + C_{k-1,n-1} \) or equivalently \( \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1} \) where the initial terms are \( C_{0,0} = 1 \), \( C_{1,0} = 0 \) and \( C_{0,1} = 1 \). Pascal’s triangle can then be defined as a triangular arrangement of the coefficients \( C_{k,n} \) over a range of values \( n \), i.e. the coefficients of an expression of the form \((1 + x)^n\).

D. Generalized Pascal’s Triangle

Now we are interested in the coefficients of the more general expression \((1 + x + x^2 + \cdots + x^{q-1})^n\). For any \( q \), we build a triangle with the same approach as in building Pascal’s triangle - by determining every coefficient in every row by summing up the \( q \) adjacent terms on top of it - which we are going to name q-ary Pascal’s triangle. This triangle and several of its identities have already been introduced in [14] and [15].

The triangle can be identified by a recurrence relation:

\[
C_{k,n}^{(q)} = \sum_{j=0}^{q-1} C_{k-j,n-1}^{(q)}
\]

where \( C_{k,n}^{(q)} \) denotes the kth coefficient in the nth row of the q-ary Pascal’s triangle and the leftmost coefficient in every row has index \( k = 0 \). Notice that in the expression \((1 + x + x^2 + \cdots + x^{q-1})^n\), the powers of \( x \) range from 0 to \( n(q-1) \), so \( 0 \leq k \leq n(q-1) \), where \( n \in \mathbb{Z}_0^+ \). Then, for any \( q \), the initial coefficients are \( C_{0,0}^{(q)} = 1 \) and \( C_{k,1}^{(q)} = 1 \) for any \( k \in \{0, 1, \ldots, (q-1)\} \). Also note that for \( q = 2 \), \( C^{(2)} \) depicts the triangular arrangement of binomial coefficients, i.e. \( C^{(2)}_{k,n} = C_{k,n} = \binom{n}{k} \).

Example. First six rows of ternary Pascal’s triangle, i.e. \( q = 3 \).
Corollary 2. For any $n$, the central coefficient in the $n$th row of a $q$-ary Pascal’s triangle is upper bounded by:

$$C_{n(q-1)/2,n}^{(q)} \leq q^{n-1}.$$  

Lemma 3. The central coefficient in the $n$th row of the $q$-ary Pascal’s triangle is upper bounded by:

$$C_{n(q-1)/2,n}^{(q)} \leq \frac{q^{n+1}}{\sqrt{n}} c_q$$

for a constant $c_q = \frac{1}{2} \left( \frac{2}{q} \right)^{q-1/2} e^{-\frac{q}{2}}$.  

E. Binary Converse Bound

We now present a converse bound on the code length $k$ for $q = 2$, i.e. for the case of constructing a query matrix $M \in \{0, 1\}^{k \times n}$ such that $\vec{u} \in \{0, 1\}^{k \times n}$ can be uniquely determined from $\vec{w} = M\vec{u} + \vec{e}$, where $\vec{e}$ is an unknown error vector with $\vec{e} \in \Z^{1 \times k}$ and $wt(\vec{e}) \leq t$, $t < k/2$.

Theorem 1 (Converse Bound). For a signature code recovering the active users in an $n$-user binary adder MAC tolerating $t$ errors it holds that

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

For the case that the amount of errors grows linearly in $k$, i.e. $t = \tau k$ with $0 \leq \tau \leq 1$, it holds that

$$k \geq \frac{2n}{(1 - \tau) \log n} - O \left( \frac{n \log \log n}{\log^2 n} \right).$$

Remark. Bshouty has already proven this bound in [5] for a fractional amount of errors $t$, but our result applies to any $t$.

Proof sketch. Define $\vec{v} \in \{0, 1\}^{1 \times n}$ to be a random binary vector taken uniformly at random. Assume $wt(\vec{u}) = m$. As $E[wt(\vec{u})] = n/2$, $E[\vec{u} \cdot \vec{v}] = m/2$. We write:

$$\Pr \left[ -\delta n \leq \vec{u} \cdot \vec{v} - \frac{m}{2} \leq +\delta n \right] \geq 1 - 2e^{-2\delta^2 n} \geq 1 - \varepsilon$$

where the inequality follows from Hoeffding’s inequality [16], $\varepsilon$ is a very small nonnegative number and $\delta$ is a nonnegative number satisfying $\delta \leq \frac{m}{2n}$. Now, define $V_1, V_2, V_3, \ldots, V_k \triangleq \{\vec{v} \in \{0, 1\}^{1 \times n} \text{ s.t. } \vec{u} \cdot \vec{v} \in \left[\frac{m}{2} - \delta n; \frac{m}{2} + \delta n\right]\}$. Also define the intersection of all these sets as $V_{\text{inter}} = \bigcap_{i=1}^{k} V_i$. Obviously, $|V_{\text{inter}}| \geq 2^n(1 - k\varepsilon)$.

When each of the $k$ queries in the query matrix $M$ is picked from their respective sets $V_i$, $i \in \{1, 2, \ldots, k\}$, every answer to every query is going to be in the interval $[\frac{m}{2} - \delta n; \frac{m}{2} + \delta n]$, so it must hold that:

$$2\delta n + 1 \leq 2^n(1 - k\varepsilon).$$

Using the Hamming ball argument on Eq (2), using $2\delta n \leq 2\delta n + 1$, and assuming $(1 - k\varepsilon) \approx 1$, we arrive at:

$$k \geq \frac{n + 2t - \frac{1}{2} \log 8t}{\log 2\delta n} + t.$$  

Set $\delta n = \sqrt{n \log n}$ and the result follows.
III. MAIN RESULTS

For the case we showed the converse bound above, we now present an explicit construction of the signature code.

**Theorem 2 (Explicit Construction).** There exists an explicit construction for signature codewords that can recover the vector of active users \( \hat{u} \) in the presence of up to \( t < k/2 \) errors for code length

\[
k \leq k_{in} + 2t \log n, \quad k_{in} = \frac{2n}{\log n} + O\left(\frac{n \log \log n}{\log^2 n}\right).
\]

**Proof sketch.** We first obtain an \( k_{in} \)-by-\( n \) query matrix \( M \) with the explicit construction presented in [3], which also shows that \( k_{in} \) queries are enough to uncover an \( n \)-bit unknown information vector. We then apply a systematic Reed-Solomon code \([n_{RS}, k_{RS}, d_{RS}]_{RS}\) on every column \( M^{(i)} \), where \( M^{(i)} \) denotes the \( i \)-th column of \( M \). As \( M^{(i)} \in \{0,1\}^{k \times 1} \), \( k_{RS} = k \). Then \( d_{RS} = n_{RS} - k_{RS} + 1 \). As \( t = \frac{2r}{2} \), \( n_{RS} = k_{RS} + 2t \). As we use \( q_{RS} \approx n \), we need a total of \( 2t \log n \) parity rows to account for \( t \) errors at the output. As a result, the newly obtained query matrix will result in such an answer sequence \( \hat{w} \) from which the noncorrupted answer vector \( \hat{w} \) can be obtained through RS decoding.

**Remark.** This theorem also applies to general \( q \), i.e. when \( M \in \{0,1,\ldots,q-1\}^{k \times n} \) for \( q \in \mathbb{Z}^+ \setminus \{1\} \) even though \( q \) does not pop up in the expression for \( k \).

**Remark.** For \( q = 2 \), there is still a significant gap between the converse bound (Theorem 1) and the explicit construction (Theorem 2). We conjecture that the construction can be improved for a constant number of errors \( t \) (not linearly growing in \( k \) and independent from \( n \) and \( k \)) as we have to increase the codeword length \( k \) by \( \log n \) for each additional error.

Now we consider general \( q \in \mathbb{Z}^+ \setminus \{1\} \), i.e. \( M \in \{0,1,\ldots,q-1\}^{k \times n} \) and \( w(M) \leq t, t < k/2 \).

We present a converse result on the parameters of signature codes for the \( q \)-ary adder MAC. This result performs better in the binary case than Theorem 1 if the number of errors is large, specifically if the fraction of errors is more than \( 1/4 \).

**Theorem 3.** There is no algorithm to construct a \( q \)-ary signature code of size \( n \) and any length \( k \) that is capable of correcting more than \( \frac{k-1}{2} q \) errors at the channel output.

**Proof sketch.** The proof follows the proof of Theorem 1 in [5] which corresponds to the case \( q = 2 \).

Toward a contradiction suppose there exists a signature code \( M \) with the required parameters. Define \( M^{(i)} \) and \( M^{(i)} \) as the \( i \)-th column and \( i \)-th row of matrix \( M \). Let \( e_i, i \in \{1,\ldots,n\} \) be the standard basis vectors of \( \mathbb{R}^n \). Define \( w_r, \ell \in \{0,1,\ldots,q-1\} \) as the number of \( 1 \)'s in \( \ell \)'s in a row vector \( M^{(i)} \). Obviously, \( \sum_{\ell=0}^{q-1} w_r = n \). Similarly define \( \gamma_\ell, \ell \in \{0,1,\ldots,q-1\} \) as the fraction of \( 1 \)'s in a row vector \( M^{(i)} \), so it follows that \( w_r = \gamma_\ell n \).

Since \( M \) tolerates \( \tau k \) incorrect answers for any \( 1 \leq i_1 < i_2 \leq n \), by Lemma 1 in [5], we have \( wt(M(e_{i_1} - e_{i_2})) = wt(M^{(i_1)} - M^{(i_2)}) > 2\tau k \). Therefore, we have

\[
\binom{n}{2} (2\tau k) < \sum_{1 \leq i_1 < i_2 \leq n} wt(M^{(i_1)} - M^{(i_2)})
= \frac{1}{2} \sum_{\ell=0}^{q-1} w_r(n - w_r)
\leq \frac{n^2}{2} \left( 1 - \frac{q-1}{q^2} \right)
\]

and we conclude that

\[
\tau < \frac{q-1}{2q} + O(1),
\]

completing the proof.

**Theorem 4 (Random Construction).** There exists an algorithm to construct a signature code of size \( n \) that detects the active users with code length \( k \), tolerating \( t \) incorrect symbols at the channel output for

\[
k > \frac{2n \log 3}{\log n + (q-1) \log \frac{3}{2}} + 2t + 1
+ O\left(\frac{n}{\log n(q + \log n)}\right).
\]

For the case that the amount of errors grows linearly in \( k \), i.e. \( t = \tau k \) with \( 0 \leq \tau \leq \frac{1}{2} - \frac{1}{4q} \), it holds that

\[
k = \frac{2n \log 3}{(1 - 2\tau) \left( \log n + (q-1) \log \frac{3}{2} \right)}
+ O\left(\frac{n}{\log n(q + \log n)}\right).
\]

**Proof sketch.** The proof of this statement is similar to the proof of Theorem 2 in [5].

Consider two different unknown information sequences \( \vec{x}, \vec{y} \in \{0,1\}^n \) and define \( \vec{z} = \vec{x} - \vec{y} \in \{1,0,1\}^n \). Our goal is to show that \( \Pr[\exists \vec{z} \in \{1,0,1\}^n : wt(M^{(i)} z) < 2t] < 1 \) which implies the result. We first upper bound the term \( \Pr[wt(M^{(i)} z) < 2t] \) by

\[
\Pr[wt(M^{(i)} z) < 2t] \leq \sum_{j=0}^{2t} \binom{2t}{j} \left( 1 - r_{w^z_r,w^z_z} \right)^j \left( r_{w^z_r,w^z_z} \right)^k.
\]

where we defined \( r_{w^z_r,w^z_z} = \Pr[M^{(i)} z = 0] \) with \( M^{(i)} \) being the \( i \)-th row in \( M \), \( w^z_r \) being the number of \( 1 \)'s in \( z \) and \( w^z_z \) being the number of \( -1 \)'s in \( z \). In order for the dot product \( M^{(i)} z \) to be equal to zero, the sum of the numbers in \( M \) whose positions coincide with \( 1 \)'s in \( z \) must be equal to the sum of the numbers in \( M \) whose positions coincide with \( -1 \)'s in \( z \). The Corollary 2 shows that the probability \( r_{w^z_r,w^z_z} \) is maximized when \( w^z_r = w^z_z = n/2 \) and Lemmas 2 and 3 help us then to upper bound \( r_{w^z_r,w^z_z} \). We then state that \( \Pr[wt(M^{(i)} z) < 2t] \leq f(q,k,t,w_z) \), where \( w_z \) is the number of nonzero positions in...
and \( f(q, k, t, w_z) \) is an expression depending on \( q, k, t, \) and \( w_z \). Then we write:

\[
\Pr(\exists z \text{wt}(MZ^T) < 2t) \leq \sum_{w_z=1}^{n} \binom{n}{w_z} 2^{w_z} f(q, k, t, w_z).
\]

We finally move on to show that for any possible tuple \((q, k, t, w_z)\)

\[
\sum_{w_z=1}^{n} \binom{n}{w_z} 2^{w_z} f(q, k, t, w_z) < \frac{1}{n}
\]

and the result follows.

Remark. We point out that Theorem 4 shows that if \( q = \mathcal{O}(n) \) the number of questions can be upper bounded by a constant \((k = \mathcal{O}(1))\) as long as \( t \leq \frac{q - 1}{2q} k \). Furthermore, it is remarkable that the random construction in Theorem 4 performs worse than the explicit construction in Theorem 2 for few errors. However, as the number of errors increases the random construction performs better than the aforementioned explicit construction.

**Theorem 5** (Explicit Construction). For a small constant \( \varepsilon > 0 \), there exists a polynomial time algorithm to construct a signature code of length

\[
k = \mathcal{O}\left(\frac{n}{\log \log n}\right)
\]

for \( n \) users that is able to correct up to \((\frac{q - 1}{2q} - \varepsilon)k\) erroneous symbols at the channel output.

*Proof sketch.* The proof follows the proof of Theorem 4 in [5].

We choose two small constants \( \varepsilon_1 \) and \( \varepsilon_2 \) such that \((\frac{q - 1}{2q} - \varepsilon_1)(1/4 - \varepsilon_2)/2 = (\frac{q - 1}{2q} - \varepsilon)\). Due to Theorem 4, there exists a query matrix \( M \in \{0, 1, \ldots, q - 1\}^{p \times s} \) that tolerates \((\frac{q - 1}{2q} - \varepsilon_1)p\) errors. For small dimensions \( p \) and \( s \), \( M \) can be found through exhaustive search.

We define \( r := n/s \) and define \( C \) as a linear code \([N, K, D] := [c_1 r, r, (1/2 - \varepsilon_2) c_1 r] \) over \( \mathbb{Z}_2 \) with \( G \in \{0, 1\}^{(1/4)c_1 r} \) and polynomial time decoding algorithm \( D \) where \( c_1 \) is a constant with \( c_1 \geq \frac{1}{2} - \frac{\varepsilon_1}{r} \). The latter is due to Singleton bound [17]. An example to such a code are concatenation codes. Let

\[
B \triangleq \tilde{G}^T \otimes M = \\
\begin{pmatrix}
g_{1,1} M & g_{1,2} M & \ldots & g_{1,r} M \\
g_{2,1} M & g_{2,2} M & \ldots & g_{2,r} M \\
\vdots & \vdots & \ddots & \vdots \\
g_{c_1 r,1} M & g_{c_1 r,2} M & \ldots & g_{c_1 r, r} M
\end{pmatrix}
\]

where \( \tilde{G} \) is essentially \( G \) but over \( \mathbb{Z} \). Note that \( B \) is a \( k \)-by-\( n \) matrix as \( rs = n \).

The matrix \( B \) tolerates \( k' = (\frac{q - 1}{2q} - \varepsilon_1)(1/4 - \varepsilon_2)/2k = (\frac{q - 1}{2q} - \varepsilon)k \) incorrect answers and given \( \tilde{v} = B\bar{v} + \bar{e} \), where \( \tilde{v} \in \{0, 1\}^n \), \( \bar{e} \in \mathbb{Z}^k \) and \( \text{wt}(\bar{e}) \leq k' \), \( \bar{v} \) can be reconstructed in polynomial time, thus the proof is complete.

**Remark.** Notice that we have presented two explicit constructions throughout this work (Theorem 2 and Theorem 5). The first one performs better if the amount of errors is small whereas it performs poorly when \( t \) is in the order of \( k_{lin} \), e.g. for \( k_{lin} = \mathcal{O}\left(\frac{n}{\log n}\right) \) it follows that \( k = \mathcal{O}(n) \). Conversely, the second construction performs poorly for small \( t \) compared to the first construction. However, for \( t \) in \( k \) the codeword length remains in \( \mathcal{O}\left(\frac{n}{\log \log n}\right) \).

**IV. Conclusion and Further Research Directions**

In this work we covered the problem of constructing signature codes for a noisy adder MAC in the adversarial setting. We have shown the existence of a set of signature codewords for the adder MAC that allow perfect detection of the active users even in the event of errors at the channel output. Specifically the paper covers the case of a fixed number of errors \( t \), independent of the amount of the signature codeword length \( k \) and the number of codewords \( n \) as well as the case that the upper bound on the number of errors is linear in \( k \), i.e. \( t = \pi k \).

Apart from the existence of signature codes we furthermore presented two explicit constructions that can be run in polynomial time with respect to \( k, n \) and \( t \). We are introducing two constructions because the first one performs better for small values of \( t \) while the latter one performs better if for large \( t \) (e.g. if \( t \) is linear in \( k \)).

Furthermore, we show a converse result, namely that it is impossible to construct signature codes for the \( q \)-ary adder MAC if the number of erroneous symbols at the channel output exceeds \((\frac{q - 1}{2q})\).

Our constructions and existence results do not match the converse bounds we present throughout this work. We conjecture that especially the first explicit construction can be improved since in the converse bound (Theorem 1) is only increased by \( 1 \) for each error while the explicit construction is increased by \( \log n \) per additional error.

An additional scenario for future work would be to consider the case that the information vector \( \tilde{u} \) is nonbinary, i.e. \( \tilde{u} \in \{0, 1, \ldots, r - 1\}^{1 \times n} \) for \( r > 2, r \in \mathbb{Z}^+ \). This case has been considered by Lindström in [3] for the error-free case. In the noisy adder MAC problem, this would translate to each user having not one, but \( r - 1 \) messages excluding the all-zero vector. In other words, each user in the channel is given a choice \( r_1 \in \{0, 1, \ldots, r - 1\} \), with which their signature codeword \( \tilde{s}_i \in \{0, 1, \ldots, q - 1\}^{r_1 \times 1} \) will be multiplied so that \( \sum_{r_1=1}^{r-1} \tilde{s}_i Y_r = Y \in \{0, 1, \ldots, n(q - 1)(r - 1)\}^{r \times 1} \). Then the goal would be to determine the vector \((r_1, r_2, \ldots, r_n)\) from \( Y \) in the presence of \( t \) errors.

**References**

[1] H. Shapiro, “Problem E 1399 in elementary problems and solutions,” *The American Mathematical Monthly*, vol. 67, no. 1, pp. 81–86, 1960.

[2] P. Erdös and A. Rényi, “On two problems of information theory,” in *Publ. Hung. Acad. Sci.*, vol. 8, 1963, pp. 241–254.

[3] B. Lindström, “On a combinatorial problem in number theory,” *Canadian Mathematical Bulletin*, vol. 8, no. 4, pp. 477–490, 1965.

[4] D. G. Cantor and W. H. Mills, “Determination of a subset from certain combinatorial properties,” *Canadian Journal of Mathematics*, vol. 18, pp. 42–48, 1966.
[5] N. Bshouty, “On the coin weighing problem with the presence of noise,” in \textit{APPROX-RANDOM}, 2012.
[6] S.-C. Chang and E. Weldon, “Coding for t-user multiple-access channels,” \textit{IEEE Transactions on Information Theory}, vol. 25, no. 6, pp. 684–691, 1979.
[7] E. van der Meulen and S. Vangheluwe, “Construction of new signature codes for the t-terminal binary adder multiple access channel with partially active users,” in \textit{International Symposium on Information Theory, 2004. ISIT 2004. Proceedings.}, 2004, pp. 107–107.
[8] V. Gritsenko, G. Kabatiansky, V. Lebedev, and A. Maevskiy, “Signature codes for noisy multiple access adder channel,” \textit{Des. Codes Cryptography}, vol. 82, no. 1–2, p. 293–299, jan 2017. [Online]. Available: https://doi.org/10.1007/s10623-016-0228-1
[9] S. András and T. Eric, “On metric generators of graphs,” \textit{Math. Oper. Res}, vol. 29, no. 2, pp. 383–393, 2004.
[10] V. Chvátal, “Mastermind,” \textit{Combinatorica}, vol. 3, pp. 325–329, 1983.
[11] G. Kabatiansky and V. Lebedev, “On metric dimension of nonbinary hamming spaces,” \textit{Problems of Information Transmission}, vol. 54, pp. 48–55, 01 2018.
[12] Z. Jiang and N. Polyanskii, “On the metric dimension of cartesian powers of a graph,” \textit{Journal of Combinatorial Theory, Series A}, vol. 165, p. 1–14, Jul 2019. [Online]. Available: http://dx.doi.org/10.1016/j.jcta.2019.01.002
[13] G. Erdőgan, G. Maringer, and N. Polyanskii, “Signature codes for a noisy adder multiple access channel,” 2022. [Online]. Available: https://arxiv.org/abs/2206.10735
[14] J. E. Freund, “Restricted occupancy theory—a generalization of pascal’s triangle,” \textit{The American Mathematical Monthly}, vol. 63, no. 1, pp. 20–27, 1956. [Online]. Available: http://www.jstor.org/stable/2308048
[15] B. Bondarenko, \textit{Generalized Pascal Triangles and Pyramids: Their Fractals, Graphs, and Applications}. Fibonacci Assoc., 1993. [Online]. Available: https://books.google.de/books?id=wyT0mwEACAAJ
[16] W. Hoeffding, “Probability inequalities for sums of bounded random variables,” \textit{Journal of the American Statistical Association}, vol. 58, no. 301, pp. 13–30, 1963. [Online]. Available: http://www.jstor.org/stable/2282952
[17] R. Singleton, “Maximum distance q-nary codes,” \textit{IEEE Trans. Inf. Theor.}, vol. 10, no. 2, p. 116–118, sep 2006. [Online]. Available: https://doi.org/10.1109/TIT.1964.1053661