Optimal Error-Detecting Codes for General Asymmetric Channels via Sperner Theory

Mladen Kovačević and Dejan Vukobratović
Faculty of Technical Sciences, University of Novi Sad, Serbia
Emails: kmladen@uns.ac.rs, dejanv@uns.ac.rs

***Abstract*—Several communication models that are of relevance in practice are asymmetric in the way they act on the transmitted "objects". Examples include channels in which the amplitudes of the transmitted pulses can only be decreased, channels in which the symbols can only be deleted, channels in which non-zero symbols can only be shifted to the right (e.g., timing channels), subspace channels in which the dimension of the transmitted vector space can only be reduced, unordered storage channels in which the cardinality of the stored (multi)set can only be reduced, etc. We introduce a formal definition of an asymmetric channel as a channel whose action induces a partial order on the set of all possible inputs, and show that this definition captures all the above examples. Such a general approach allows one to treat all these different models in a unified way, and to obtain a characterization of optimal error-detecting codes for many interesting asymmetric channels by using Sperner theory.**

I. Introduction

Several important channel models possess an intrinsic asymmetry in the way they act on the transmitted "objects". A classical example is the binary Z-channel in which the transmitted 1's may be received as 0's, but not vice versa. In this article we formalize the notion of an asymmetric channel by using order theory, and illustrate that the given definition captures this and many more examples. Our main goals are the following: 1) to introduce a framework that enables one to treat many different kinds of asymmetric channels in a unified way, and 2) to demonstrate its usefulness and meaningfulness through examples. In particular, the usefulness of the framework is illustrated by describing *optimal* error-detecting codes for a broad class of asymmetric channels (for all channel parameters), a result that follows from Kleitman's theorem on posets satisfying the so-called LYM inequality.

A. Communication channels

Definition 1. *Let $\mathcal{X}, \mathcal{Y}$ be nonempty sets. A communication channel on $(\mathcal{X}, \mathcal{Y})$ is a subset $\mathcal{K} \subseteq \mathcal{X} \times \mathcal{Y}$ satisfying $\forall x \in \mathcal{X}\ \exists y \in \mathcal{Y}\ (x, y) \in \mathcal{K}$ and $\forall y \in \mathcal{Y}\ \exists x \in \mathcal{X}\ (x, y) \in \mathcal{K}$. We also use the notation $x \overset{\mathcal{K}}{\rightsquigarrow} y$, or simply $x \rightsquigarrow y$ when there is no risk of confusion, for $(x, y) \in \mathcal{K}$.*

For a given channel $\mathcal{K} \subseteq \mathcal{X} \times \mathcal{Y}$, we define its dual channel as $\mathcal{K}^{\mathrm{d}} = \{(y, x) : (x, y) \in \mathcal{K}\}$.

Note that we describe communication channels purely in combinatorial terms, as *relations* in Cartesian products $\mathcal{X} \times \mathcal{Y}$. Here $\mathcal{X}$ is thought of as the set of all possible inputs, and $\mathcal{Y}$ as the set of all possible outputs of the channel. The expression $x \rightsquigarrow y$ means that the input x can produce the output y with positive probability. We do not assign particular values of probabilities to each pair $(x, y) \in \mathcal{K}$ as they are irrelevant for the problems that we intend to discuss.

B. Partially ordered sets

In what follows, we shall use several notions from order theory, so we recall the basics here [6], [20].

A partially ordered set (or poset) is a set $\mathcal{U}$ together with a relation $\preceq$ satisfying, for all $x, y, z \in \mathcal{U}$: 1) reflexivity: $x \preceq x$, 2) asymmetry (or antisymmetry): if $x \preceq y$ and $y \preceq x$, then $x = y$, 3) transitivity: if $x \preceq y$ and $y \preceq z$, then $x \preceq z$. Two elements $x, y \in \mathcal{U}$ are said to be comparable if either $x \preceq y$ or $y \preceq x$. They are said to be incomparable otherwise. A chain in a poset $(\mathcal{U}, \preceq)$ is a subset of $\mathcal{U}$ in which any two elements are comparable. An antichain is a subset of $\mathcal{U}$ any two distinct elements of which are incomparable.

A function $\rho : \mathcal{U} \to \mathbb{N}$ is called a rank function if $\rho(y) = \rho(x) + 1$ whenever y covers x, meaning that $x \preceq y$ and there is no $y' \in \mathcal{U}$ such that $x \preceq y' \preceq y$. A poset with a rank function is called graded. In a graded poset with rank function ρ we denote $\mathcal{U}_{[\underline{\ell}, \overline{\ell}]} = \{x \in \mathcal{U} : \underline{\ell} \leqslant \rho(x) \leqslant \overline{\ell}\}$, and we also write $\mathcal{U}_{\ell} = \mathcal{U}_{[\ell, \ell]}$ (here the rank function ρ is omitted from the notation as it is usually understood from the context). Hence, $\mathcal{U} = \bigcup_{\ell} \mathcal{U}_{\ell}$. A graded poset is said to have Sperner property if $\mathcal{U}_{\ell}$ is an antichain of maximum cardinality in $(\mathcal{U}, \preceq)$, for some ℓ. A poset is called rank-unimodal if the sequence $|\mathcal{U}_{\ell}|$ is unimodal (i.e., an increasing function of ℓ when $\ell \leqslant \ell'$, and decreasing when $\ell \geqslant \ell'$, for some ℓ').

We say that a graded poset $(\mathcal{U}, \preceq)$ possesses the LYM (Lubell–Yamamoto–Meshalkin) property [11] if there exists a nonempty list of maximal chains such that, for any ℓ, each of the elements of rank ℓ appear in the same number of chains. In other words, if there are L chains in the list, then each element of rank ℓ appears in $L/|\mathcal{U}_{\ell}|$ of the chains. We shall call a poset *normal* if it satisfies the LYM property, see [6, Sec. 4.5 and Thm 4.5.1]. A simple sufficient condition for a poset to be normal is that it be regular [6, Cor. 4.5.2], i.e., that both the number of elements that cover x and the number of elements that are covered by x depend only on the rank of x.

In Section III we shall see that many standard examples of posets, including the Boolean lattice, the subspace lattice, the Young's lattice, chain products, etc., arise naturally in the analysis of communications channels.

II. General asymmetric channels and error-detecting codes

In this section we give a formal definition of asymmetric channels and the corresponding codes which unifies and generalizes many scenarios analyzed in the literature. We assume hereafter that the sets of all possible channel inputs and all possible channels outputs are equal, $\mathcal{X} = \mathcal{Y}$.

For a very broad class of communication channels, the relation $\rightsquigarrow$ is reflexive, i.e., $x \rightsquigarrow x$ (any channel input can be received unimpaired, in case there is no noise), and transitive, i.e., if $x \rightsquigarrow y$ and $y \rightsquigarrow z$, then $x \rightsquigarrow z$ (if there is a noise pattern that transforms x into y, and a noise pattern that transforms y into z, then there is a noise pattern – a combination of the two – that transforms x into z). Given such a channel, we say that it is *asymmetric* if the relation $\rightsquigarrow$ is asymmetric, i.e., if $x \rightsquigarrow y$, $x \neq y$, implies that $y \not\rightsquigarrow x$. In other words, we call a channel asymmetric if the channel action induces a partial order on the space of all inputs $\mathcal{X}$.

Definition 2. *A communication channel $\mathcal{K} \subseteq \mathcal{X}^2$ is said to be asymmetric if $(\mathcal{X}, \overset{\mathcal{K}}{\rightsquigarrow})$ is a partially ordered set. We say that such a channel is * if the poset $(\mathcal{X}, \overset{\mathcal{K}}{\rightsquigarrow})$ is *, where * stands for an arbitrary property a poset may have (e.g., graded, Sperner, normal, etc.).*

Many asymmetric channels that arise in practice, including all the examples mentioned in this paper, are graded as there are natural rank functions that may be assigned to them. For a graded channel $\mathcal{K}$, we denote by $\mathcal{K}_{[\underline{\ell},\overline{\ell}]} = \mathcal{K} \cap \big(\mathcal{X}_{[\underline{\ell},\overline{\ell}]}\big)^2$ its natural restriction to inputs of rank $\underline{\ell}, \ldots, \overline{\ell}$.

Definition 3. *We say that $\boldsymbol{C} \subseteq \mathcal{X}$ is a code detecting up to t errors in a graded asymmetric channel $\mathcal{K} \subseteq \mathcal{X}^2$ if, for all $x, y \in \boldsymbol{C}$,*

$$x \overset{\mathcal{K}}{\rightsquigarrow} y \,\wedge\, x \neq y \quad \Rightarrow \quad |\operatorname{rank}(x) - \operatorname{rank}(y)| > t. \tag{1}$$

We say that $\boldsymbol{C} \subseteq \mathcal{X}$ detects all *error patterns in an asymmetric channel $\mathcal{K} \subseteq \mathcal{X}^2$ if, for all $x, y \in \boldsymbol{C}$,*

$$x \overset{\mathcal{K}}{\rightsquigarrow} y \quad \Rightarrow \quad x = y. \tag{2}$$

For graded channels, the condition (2) is satisfied if and only if the condition (1) holds for any t.

In words, $\boldsymbol{C}$ detects all error patterns in a given asymmetric channel if no element of $\boldsymbol{C}$ can produce another element of $\boldsymbol{C}$ at the channel output. If this is the case, the receiver will easily recognize whenever the transmission is erroneous because the received object is not going to be a valid codeword which could have been transmitted. Yet another way of saying that $\boldsymbol{C}$ detects all error patterns is the following.

Proposition 4. *$\boldsymbol{C} \subseteq \mathcal{X}$ detects all error patterns in an asymmetric channel $\mathcal{K} \subseteq \mathcal{X}^2$ if and only if $\boldsymbol{C}$ is an antichain in the corresponding poset $(\mathcal{X}, \overset{\mathcal{K}}{\rightsquigarrow})$.*

A simple example of an antichain, and hence a code detecting all error patterns in a graded asymmetric channel, is the level set $\mathcal{X}_\ell$, for an arbitrary ℓ.

Definition 5. *We say that $\boldsymbol{C} \subseteq \mathcal{X}$ is an optimal code detecting up to t errors (resp. all error patterns) in a graded asymmetric channel $\mathcal{K} \subseteq \mathcal{X}^2$ if there is no code of cardinality larger than $|\boldsymbol{C}|$ that satisfies* (1) *(resp.* (2)*).*

Hence, an optimal code detecting all error patterns in an asymmetric channel $\mathcal{K} \subseteq \mathcal{X}^2$ is an antichain of maximum cardinality in the poset $(\mathcal{X}, \overset{\mathcal{K}}{\rightsquigarrow})$. Channels in which the code $\mathcal{X}_\ell$ is optimal, for some ℓ, are called Sperner channels. All channels treated in this paper are Sperner.

An example of an error-detecting code, of which the code $\mathcal{X}_\ell$ is a special case (obtained for $t \to \infty$), is given in the following proposition.

Proposition 6. *Let $\mathcal{K} \subseteq \mathcal{X}^2$ be a graded asymmetric channel, and $(\ell_n)_n$ a sequence of integers satisfying $\ell_n - \ell_{n-1} > t$, $\forall n$. The code $\boldsymbol{C} = \bigcup_n \mathcal{X}_{\ell_n}$ detects up to t errors in $\mathcal{K}$.*

If the channel is normal, an optimal code detecting up to t errors is of the form given in Proposition 6. We state this fact for channels which are additionally rank-unimodal, as this is the case that is most common.

Theorem 7. *Let $\mathcal{K} \subseteq \mathcal{X}^2$ be a normal rank-unimodal asymmetric channel. The maximum cardinality of a code detecting up to t errors in $\mathcal{K}_{[\underline{\ell},\overline{\ell}]}$ is given by*

$$\max_{m} \sum_{\substack{\ell=\underline{\ell} \\ \ell \equiv m \pmod{t+1}}}^{\overline{\ell}} |\mathcal{X}_\ell|. \tag{3}$$

Proof: This is essentially a restatement of the result of Kleitman [11] (see also [6, Cor. 4.5.4]) which states that, in a finite normal poset $(\mathcal{U}, \preceq)$, the largest cardinality of a family $\boldsymbol{C} \subseteq \mathcal{U}$ having the property that, for all distinct $x, y \in \boldsymbol{C}$, $x \preceq y$ implies that $\operatorname{rank}(y) - \operatorname{rank}(x) > t$, is $\max_F \sum_{x \in F} |\mathcal{U}_{\operatorname{rank}(x)}|$. The maximum here is taken over all chains $F = \{x_1, x_2, \ldots, x_c\}$ satisfying $x_1 \preceq x_2 \preceq \cdots \preceq x_c$ and $\operatorname{rank}(x_{i+1}) - \operatorname{rank}(x_i) > t$ for $i = 1, 2, \ldots, c-1$, and all $c = 1, 2, \ldots$. If the poset $(\mathcal{U}, \preceq)$ is in addition rank-unimodal, then it is easy to see that the maximum is attained for a chain F satisfying $\operatorname{rank}(x_{i+1}) - \operatorname{rank}(x_i) = t+1$ for $i = 1, 2, \ldots, c-1$, and that the maximum cardinality of a family $\boldsymbol{C}$ having the stated property can therefore be written in the simpler form

$$\max_{m} \sum_{\ell \equiv m \pmod{t+1}} |\mathcal{U}_\ell|. \tag{4}$$

Finally, (3) follows by recalling that the restriction $(\mathcal{U}_{[\underline{\ell},\overline{\ell}]}, \preceq)$ of a normal poset $(\mathcal{U}, \preceq)$ is normal [6, Prop. 4.5.3]. ■

We note that an optimal value of m in (3) can be determined explicitly in many concrete examples (see Section III).

We conclude this section with the following claim which enables one to directly apply the results pertaining to a given asymmetric channel to its dual.

Proposition 8. *A channel $\mathcal{K} \subseteq \mathcal{X}^2$ is asymmetric if and only if its dual $\mathcal{K}^{\mathrm{d}}$ is asymmetric. A code $\boldsymbol{C} \subseteq \mathcal{X}$ detects up to t errors in $\mathcal{K}$ if and only if it detects up to t errors in $\mathcal{K}^{\mathrm{d}}$.*

III. EXAMPLES

In this section we list several examples of communication channels that have been analyzed in the literature in different contexts and that are asymmetric in the sense of Definition 2. For each of them, a characterization of optimal error-detecting codes is given based on Theorem 7.

A. Codes in power sets

Consider a communication channel with $\mathcal{X} = \mathcal{Y} = 2^{\{1,\dots,n\}}$ and with $A \rightsquigarrow B$ if and only if $B \subseteq A$, where $A, B \subseteq \{1,\dots,n\}$. Codes defined in the power set $2^{\{1,\dots,n\}}$ were proposed in [8], [15] for error control in networks that randomly reorder the transmitted packets (where the set $\{1,\dots,n\}$ is identified with the set of all possible packets), and are also of interest in scenarios where data is written in an unordered way, such as DNA-based data storage systems [17]. Our additional assumption here is that the received set is always a subset of the transmitted set, i.e., the noise is represented by "set reductions". These kinds of errors may be thought of as consequences of packet losses/deletions. Namely, if t packets from the transmitted set A are lost in the channel, then the received set B will be a subset of A of cardinality $|A| - t$. We are interested in codes that are able to detect up to t packet deletions, i.e., codes having the property that if $B \subsetneq A$, $|A| - |B| \leqslant t$, then A and B cannot both be codewords.

It is easy to see that the above channel is asymmetric in the sense of Definition 2; the "asymmetry" in this model is reflected in the fact that the cardinality of the transmitted set can only be reduced. The poset $(\mathcal{X}, \rightsquigarrow)$ is the so-called Boolean lattice [6, Ex. 1.3.1]. The rank function associated with it is the set cardinality: $\operatorname{rank}(A) = |A|$, for any $A \subseteq \{1,\dots,n\}$. This poset is rank-unimodal, with $|\mathcal{X}_\ell| = \binom{n}{\ell}$, and normal [6, Ex. 4.6.1]. By applying Theorem 7 we then obtain the maximum cardinality of a code $\boldsymbol{C} \subseteq 2^{\{1,\dots,n\}}$ detecting up to t deletions. Furthermore, an optimal value of m in (3) can be found explicitly in this case. This claim was first stated by Katona [10] in a different terminology.

Theorem 9. *The maximum cardinality of a code $\boldsymbol{C} \subseteq 2^{\{1,\dots,n\}}$ detecting up to t deletions is*

$$\sum_{\substack{\ell=0 \\ \ell \equiv \lfloor \frac{n}{2} \rfloor \ (\mathrm{mod}\ t+1)}}^{n} \binom{n}{\ell} \tag{5}$$

Setting $t \to \infty$ (in fact, $t > \lceil n/2 \rceil$ is sufficient), we conclude that the maximum cardinality of a code detecting any number of deletions is $\binom{n}{\lfloor n/2 \rfloor} = \binom{n}{\lceil n/2 \rceil}$. This is a restatement of the well-known Sperner's theorem [19], [6, Thm 1.1.1].

For the above channel, its dual (see Definition 1) is the channel with $\mathcal{X} = 2^{\{1,\dots,n\}}$ in which $A \rightsquigarrow B$ if and only if $B \supseteq A$. This kind of noise, "set augmentation", may be thought of as a consequence of packet insertions. Proposition 8 implies that the expression in (5) is also the maximum cardinality of a code $\boldsymbol{C} \subseteq \mathcal{X}$ detecting up to t insertions.

B. Codes in the space of multisets

A natural generalization of the model from the previous subsection, also motivated by unordered storage or random permutation channels, is obtained by allowing repetitions of symbols, i.e., by allowing the codewords to be *multisets* over a given alphabet [14].

A multiset A over $\{1,\dots,n\}$ can be uniquely described by its multiplicity vector $\mu_A = (\mu_A(1),\dots,\mu_A(n)) \in \mathbb{N}^n$, where $\mathbb{N} = \{0,1,\dots\}$. Here $\mu_A(i)$ is the number of occurrences of the symbol $i \in \{1,\dots,n\}$ in A. We again consider the deletion channel in which $A \rightsquigarrow B$ if and only if $B \subseteq A$ or, equivalently, if $\mu_B \leqslant \mu_A$ (coordinate wise).

If we agree to use the multiplicity vector representation of multisets, we may take $\mathcal{X} = \mathcal{Y} = \mathbb{N}^n$. The channel just described is asymmetric in the sense of Definition 2. The rank function associated with the poset $(\mathcal{X}, \rightsquigarrow)$ is the multiset cardinality: $\operatorname{rank}(A) = \sum_{i=1}^n \mu_A(i)$. We have $|\mathcal{X}_\ell| = \binom{\ell+n-1}{n-1}$.

The following claim is a multiset analog of Theorem 9.

Theorem 10. *The maximum cardinality of a code $\boldsymbol{C} \subseteq \mathcal{X}_{[\underline{\ell},\overline{\ell}]}$, $\mathcal{X} = \mathbb{N}^n$, detecting up to t deletions is*

$$\sum_{i=0}^{\lfloor \frac{\overline{\ell}-\underline{\ell}}{t+1} \rfloor} \binom{\overline{\ell} - i(t+1) + n - 1}{n-1}. \tag{6}$$

Proof: The poset $(\mathcal{X}, \rightsquigarrow)$ is normal as it is a product of chains [6, Ex. 4.6.1]. We can therefore apply Theorem 7. Furthermore, since $|\mathcal{X}_\ell| = \binom{\ell+n-1}{n-1}$ is a monotonically increasing function of ℓ, the optimal choice of m in (3) is $\overline{\ell}$, which implies (6). ■

The dual channel is the channel in which $A \rightsquigarrow B$ if and only if $B \supseteq A$, i.e., $\mu_B \geqslant \mu_A$. These kinds of errors – multiset augmentations – may be caused by insertions or duplications.

C. Codes for the binary Z*-channel and its generalizations*

Another interpretation of Katona's theorem [10] in the coding-theoretic context, easily deduced by identifying subsets of $\{1,\dots,n\}$ with sequences in $\{0,1\}^n$, is the following: the expression in (5) is the maximum size of a binary code of length n detecting up to t asymmetric errors, i.e., errors of the form $1 \to 0$ [4]. By using Kleitman's result [11], Borden [4] also generalized this statement and described optimal codes over arbitrary alphabets detecting t asymmetric errors. (Error control problems in these kinds of channels have been studied quite extensively; see, e.g., [3], [5].)

To describe the channel in more precise terms, we take $\mathcal{X} = \mathcal{Y} = \{0,1,\dots,a-1\}^n$ and we let $(x_1,\dots,x_n) \rightsquigarrow (y_1,\dots,y_n)$ if and only if $y_i \leqslant x_i$ for all $i = 1,\dots,n$. This channel is asymmetric and the poset $(\mathcal{X}, \rightsquigarrow)$ is normal [6, Ex. 4.6.1]. The appropriate rank function here is the Manhattan weight: $\operatorname{rank}(x_1,\dots,x_n) = \sum_{i=1}^n x_i$. In the binary case ($a = 2$), this channel is called the Z-channel and the Manhattan weight coincides with the Hamming weight.

Let $c(N, M, \ell)$ denote the number of *compositions* of the number ℓ with M non-negative parts, each part being $\leqslant N$ [2, Sec. 4.2]. In other words, $c(N, M, \ell)$ is the number of vectors from $\{0,1,\ldots,N-1\}^M$ having Manhattan weight ℓ. Restricted integer compositions are well-studied objects; for an explicit expression for $c(N,M,\ell)$, see [20, p. 307].

Theorem 11 (Borden [4])**.** *The maximum cardinality of a code $\boldsymbol{C} \subseteq \{0,1,\ldots,a-1\}^n$ detecting up to t asymmetric errors is*

$$\sum_{\substack{\ell=0 \\ \ell \equiv \lfloor \frac{n(a-1)}{2} \rfloor \ (\mathrm{mod}\ t+1)}}^{n(a-1)} c(a-1,n,\ell). \tag{7}$$

The channel dual to the one described above is the channel in which $(x_1,\ldots,x_n) \rightsquigarrow (y_1,\ldots,y_n)$ if and only if $y_i \geqslant x_i$ for all $i=1,\ldots,n$.

D. Subspace codes

Let $\mathbb{F}_q$ denote the field of q elements, where q is a prime power, and $\mathbb{F}_q^n$ an n-dimensional vector space over $\mathbb{F}_q$. Denote by $\mathcal{P}_q(n)$ the set of all subspaces of $\mathbb{F}_q^n$ (also known as the projective space), and by $\mathcal{G}_q(n,\ell)$ the set of all subspaces of dimension ℓ (also known as the Grassmannian). The cardinality of $\mathcal{G}_q(n,\ell)$ is expressed through the q-binomial (or Gaussian) coefficients [21, Ch. 24]:

$$|\mathcal{G}_q(n,\ell)| = \binom{n}{\ell}_q = \prod_{i=0}^{\ell-1} \frac{q^{n-i}-1}{q^{\ell-i}-1}. \tag{8}$$

The following well-known properties of $\binom{n}{\ell}_q$ will be useful: 1) symmetry: $\binom{n}{\ell}_q = \binom{n}{n-\ell}_q$, and 2) unimodality: $\binom{n}{\ell}_q$ is increasing in ℓ for $\ell \leqslant \frac{n}{2}$, and decreasing for $\ell \geqslant \frac{n}{2}$. We use the convention that $\binom{n}{\ell}_q = 0$ when $\ell < 0$ or $\ell > n$.

Codes in $\mathcal{P}_q(n)$ were proposed in [16] for error control in networks employing random linear network coding [9], in which case $\mathbb{F}_q^n$ corresponds to the set of all length-n packets (over a q-ary alphabet) that can be exchanged over the network links. We consider a channel model in which the only impairments are "dimension reductions", meaning that, for any given transmitted vector space $U \subseteq \mathbb{F}_q^n$, the possible channel outputs are subspaces of U. These kinds of errors can be caused by packet losses, unfortunate choices of the coefficients in the performed linear combinations in the network (resulting in linearly dependent packets at the receiving side), etc.

In the notation introduced earlier, we set $\mathcal{X} = \mathcal{Y} = \mathcal{P}_q(n)$ and define the channel by: $U \rightsquigarrow V$ if and only if V is a subspace of U. This channel is asymmetric. The poset $(\mathcal{X}, \rightsquigarrow)$ is the so-called linear lattice (or the subspace lattice) [6, Ex. 1.3.9]. The rank function associated with it is the dimension of a vector space: $\operatorname{rank}(U) = \dim U$, for $U \in \mathcal{P}_q(n)$. We have $|\mathcal{X}_\ell| = |\mathcal{G}_q(n,\ell)| = \binom{n}{\ell}_q$.

The following statement may be seen as the q-analog [21, Ch. 24] of Katona's theorem [10], or of Theorem 9.

Theorem 12. *The maximum cardinality of a code $\boldsymbol{C} \subseteq \mathcal{P}_q(n)$ detecting dimension reductions of up to t is*

$$\sum_{\substack{\ell=0 \\ \ell \equiv \lfloor \frac{n}{2} \rfloor \ (\mathrm{mod}\ t+1)}}^{n} \binom{n}{\ell}_q. \tag{9}$$

Proof: The poset $(\mathcal{P}_q(n), \subseteq)$ is rank-unimodal and normal [6, Ex. 4.5.1] and hence, by Theorem 7, the maximum cardinality of a code detecting dimension reductions of up to t can be expressed in the form

$$\max_m \sum_{\substack{\ell=0 \\ \ell \equiv m \ (\mathrm{mod}\ t+1)}}^{n} \binom{n}{\ell}_q \tag{10a}$$

$$= \max_{r \in \{0,1,\ldots,t\}} \sum_{j \in \mathbb{Z}} \binom{n}{\lfloor \frac{n}{2} \rfloor + r + j(t+1)}_q. \tag{10b}$$

(Expression (10a) was also given in [1, Thm 7].) We need to show that $m = \lfloor n/2 \rfloor$ is a maximizer in (10a) or, equivalently, that $r = 0$ is a maximizer in (10b). Let us assume for simplicity that n is even; the proof for odd n is similar. What we need to prove is that the following expression is non-negative, for any $r \in \{1,\ldots,t\}$,

$$\sum_{j \in \mathbb{Z}} \binom{n}{\frac{n}{2} + j(t+1)}_q - \sum_{j \in \mathbb{Z}} \binom{n}{\frac{n}{2} + r + j(t+1)}_q$$

$$= \sum_{j>0} \binom{n}{\frac{n}{2} + j(t+1)}_q - \binom{n}{\frac{n}{2} + r + j(t+1)}_q + \tag{11a}$$

$$\binom{n}{\frac{n}{2}}_q - \binom{n}{\frac{n}{2} + r}_q - \binom{n}{\frac{n}{2} + r - (t+1)}_q + \tag{11b}$$

$$\sum_{j<0} \binom{n}{\frac{n}{2} + j(t+1)}_q - \binom{n}{\frac{n}{2} + r + (j-1)(t+1)}_q. \tag{11c}$$

Indeed, since the q-binomial coefficients are unimodal and maximized at $\ell = n/2$, each of the summands in the sums (11a) and (11c) is non-negative, and the expression in (11b) is also non-negative because

$$\binom{n}{\frac{n}{2}}_q - \binom{n}{\frac{n}{2} + r}_q - \binom{n}{\frac{n}{2} + r - (t+1)}_q$$

$$\geqslant \binom{n}{\frac{n}{2}}_q - \binom{n}{\frac{n}{2} + 1}_q - \binom{n}{\frac{n}{2} - 1}_q \tag{12a}$$

$$= \binom{n}{\frac{n}{2}}_q - 2\binom{n}{\frac{n}{2} - 1}_q \tag{12b}$$

$$= \binom{n}{\frac{n}{2}}_q \left(1 - 2\frac{q^{\frac{n}{2}+1}-1}{q^{\frac{n}{2}+2}-1}\right) \tag{12c}$$

$$> \binom{n}{\frac{n}{2}}_q \left(1 - 2\frac{1}{q}\right) \tag{12d}$$

$$\geqslant 0, \tag{12e}$$

where (12a) and (12b) follow from unimodality and symmetry of $\binom{n}{\ell}_q$, (12c) is obtained by substituting the definition of $\binom{n}{\ell}_q$, (12d) follows from the fact that $\frac{\alpha-1}{\beta-1} < \frac{\alpha}{\beta}$ when $1 < \alpha < \beta$, and (12e) is due to $q \geqslant 2$. ■

As a special case when $t \to \infty$ (in fact, $t > \lceil n/2 \rceil$ is sufficient), we conclude that the maximum cardinality of a code detecting arbitrary dimension reductions is $\binom{n}{\lfloor n/2 \rfloor}_q$. In other words, $\mathcal{G}_q(n, \lfloor n/2 \rfloor)$ is an antichain of maximum cardinality in the poset $(\mathcal{P}_q(n), \subseteq)$ (see Prop. 4). This is the well-known q-analog of Sperner's theorem [21, Thm 24.1].

The dual channel in this example is the channel in which $U \rightsquigarrow V$ if and only if U is a subspace of V.

E. Codes for deletion and insertion channels

Consider the channel with $\mathcal{X} = \mathcal{Y} = \{0, 1, \ldots, a-1\}^* = \bigcup_{n=0}^{\infty} \{0, 1, \ldots, a-1\}^n$ in which $x \rightsquigarrow y$ if and only if y is a subsequence of x. This is the so-called deletion channel in which the output sequence is produced by deleting some of the symbols of the input sequence. The channel is asymmetric in the sense of Definition 2. The rank function associated with the poset $(\mathcal{X}, \rightsquigarrow)$ is the sequence length: for any $x = x_1 \cdots x_\ell$, where $x_i \in \{0, 1, \ldots, a-1\}$, $\operatorname{rank}(x) = \ell$. We have $|\mathcal{X}_\ell| = a^\ell$.

Given that $\mathcal{X}$ is infinite, we shall formulate the following statement for the restriction $\mathcal{X}_{[\underline{\ell}, \overline{\ell}]}$, i.e., under the assumption that only sequences of lengths $\underline{\ell}, \ldots, \overline{\ell}$ are allowed as inputs. This is a reasonable assumption from the practical viewpoint.

Theorem 13. *The maximum cardinality of a code $\boldsymbol{C} \subseteq \bigcup_{\ell=\underline{\ell}}^{\overline{\ell}} \{0, 1, \ldots, a-1\}^\ell$ detecting up to t deletions is*

$$\sum_{j=0}^{\lfloor \frac{\overline{\ell}-\underline{\ell}}{t+1} \rfloor} a^{\overline{\ell}-j(t+1)}. \tag{13}$$

Proof: The poset $(\mathcal{X}_{[0,\overline{\ell}]}, \rightsquigarrow)$ is normal. To see this, note that the list of $a^{\overline{\ell}}$ maximal chains of the form $\epsilon \rightsquigarrow x_1 \rightsquigarrow x_1 x_2 \rightsquigarrow \cdots \rightsquigarrow x_1 x_2 \ldots x_{\overline{\ell}}$, where ϵ is the empty sequence and $x_i \in \{0, 1, \ldots, a-1\}$, satisfies the condition that each element of $\mathcal{X}_{[0,\overline{\ell}]}$ of rank ℓ appears in the same number of chains, namely $a^{\overline{\ell}-\ell}$ (see Section I-B). The claim now follows by invoking Theorem 7 and by using the fact that $|\mathcal{X}_\ell| = a^\ell$ is a monotonically increasing function of ℓ, implying that the optimal choice for m in (3) is $\overline{\ell}$. ■

The dual channel in this example is the insertion channel in which $x \rightsquigarrow y$ if and only if x is a subsequence of y.

F. Codes for bit-shift and timing channels

Let $\mathcal{X} = \mathcal{Y} = \{0, 1\}^n$, and let us describe binary sequences by specifying the positions of 1's in them. More precisely, we identify $x \in \{0, 1\}^n$ with the integer sequence $\lambda_x = (\lambda_x(1), \ldots, \lambda_x(w))$, where $\lambda_x(i)$ is the position of the i'th 1 in x, and w is the Hamming weight of x. This sequence satisfies $1 \leqslant \lambda_x(1) < \lambda_x(2) < \cdots < \lambda_x(w) \leqslant n$. For example, for $x = 1100101$, $\lambda_x = (1, 2, 5, 7)$. In fact, it will be more convenient to use a slightly different description of a sequence x, namely $\tilde{\lambda}_x = \lambda_x - (1, 2, \ldots, w)$, for which it holds that $0 \leqslant \tilde{\lambda}_x(1) \leqslant \tilde{\lambda}_x(2) \leqslant \cdots \leqslant \tilde{\lambda}_x(w) \leqslant n - w$.

Consider a communication model in which each of the 1's in the input sequence may be shifted to the right [18], [12]. Such models are also useful for describing timing channels wherein 1's indicate the time slots in which packets have been sent and shifts of these 1's are consequences of packet delays; see for example [13]. Thus $x \rightsquigarrow y$ if and only if x and y have the same Hamming weight and $\lambda_x \leqslant \lambda_y$ (coordinate wise). Since a necessary condition for $x \rightsquigarrow y$ is that x and y have the same Hamming weight, we may consider the sets of inputs $\{0, 1\}^n_w \equiv \{x \in \{0, 1\}^n : \sum_{i=1}^n x_i = w\}$ separately, for each $w = 0, \ldots, n$ (here $x = x_1 \cdots x_n$).

The above channel is asymmetric. The poset $(\{0, 1\}^n_w, \rightsquigarrow)$ is denoted $L(n-w, w)$ in [6, Ex. 1.3.13]. The rank function on this poset is defined by: $\operatorname{rank}(x) = \sum_{i=1}^w \tilde{\lambda}_x(i)$, where w is the Hamming weight of x.

Let $p(N, M, \ell)$ denote the number of *partitions* of the number ℓ into at most M positive parts, each part being $\leqslant N$ [2, Sec. 3.2]. These too are very well-studied objects. An interesting connection between them and the Gaussian coefficients which we encountered in Section III-D is the following [2, Sec. 3.2], [21, Thm 24.2]:

$$\sum_{\ell=0}^{MN} p(N, M, \ell) q^\ell = \binom{N+M}{M}_q. \tag{14}$$

Theorem 14. *The maximum cardinality of a code $\boldsymbol{C} \subseteq \{0, 1\}^n_w$ detecting up to t right-shifts is lower-bounded by*

$$\sum_{\substack{\ell=0 \\ \ell \equiv \lfloor \frac{w(n-w)}{2} \rfloor \ (\mathrm{mod}\ t+1)}}^{w(n-w)} p(n-w, w, \ell). \tag{15}$$

The maximum cardinality of a code $\boldsymbol{C} \subseteq \{0, 1\}^n_w$ detecting all patterns of right-shifts is $p(n-w, w, \lfloor \frac{w(n-w)}{2} \rfloor)$.

Proof: The number of elements in $\{0, 1\}^n_w$ of rank ℓ is $p(n-w, w, \ell)$. These numbers are symmetric, $p(n-w, w, \ell) = p(n-w, w, w(n-w)-\ell)$, and unimodal, and hence maximized when $\ell = \lfloor \frac{w(n-w)}{2} \rfloor$ [2, Thm 3.10]. Furthermore, it follows from [6, Thm 6.2.10 and Cor. 6.2.1] that the poset $(\{0, 1\}^n_w, \rightsquigarrow)$ is Sperner. This implies the second statement. The first statement follows from Proposition 6. ■

We believe the lower bound in (15) is actually the optimal value, i.e., the maximum cardinality of a code detecting t right-shifts, but at present we do not have a proof of this fact.

The dual channel in this example is the channel in which non-zero symbols may be shifted only to the left.

IV. CONCLUSION

As we have seen, order theory is a powerful tool for analyzing asymmetric channel models, particularly the error detection problem for which an optimal solution may be obtained in many cases of interest. Developing the introduced framework further and exploring other applications and channel models that fit into it is a topic of ongoing investigation.

Note that we have not discussed here error-*correcting* codes in the posets we encountered. This is also left for future work (see [7] for a related study).

Acknowledgment: This work was supported by European Union's Horizon 2020 research and innovation programme (Grant Agreement no. 856967), and by the Secretariat for Higher Education and Scientific Research of the Autonomous Province of Vojvodina (project no. 142-451-2686/2021).

References

[1] R. Ahlswede and H. Aydinian, "On Error Control Codes for Random Network Coding," in *Proc. Workshop on Network Coding, Theory and Applications (NetCod)*, pp. 68–73, Lausanne, Switzerland, June 2009.

[2] G. E. Andrews, *The Theory of Partitions*, Addison-Wesley Publishing Company, 1976.

[3] M. Blaum, *Codes for Detecting and Correcting Unidirectional Errors*, IEEE Computer Society Press, 1993.

[4] J. M. Borden, "Optimal Asymmetric Error Detecting Codes," *Inform. and Control*, vol. 53, no. 1-2, pp. 66–73, 1982.

[5] B. Bose and T. R. N. Rao, "Theory of Unidirectional Error Correcting/Detecting Codes," *IEEE Trans. Comput.*, vol. 31, no. 6, pp. 521–530, 1982.

[6] K. Engel, *Sperner Theory*, Cambridge University Press, 1997.

[7] M. Firer, M. M. S. Alves, J. A. Pinheiro, and L. Panek, *Poset Codes: Partial Orders, Metrics and Coding Theory*, Springer, 2018.

[8] M. Gadouleau and A. Goupil, "A Matroid Framework for Noncoherent Random Network Communications," *IEEE Trans. Inform. Theory*, vol. 57, no. 2, pp. 1031–1045, 2011.

[9] T. Ho, M. Médard, R. Kötter, D. Karger, M. Effros, J. Shi, and B. Leong, "A Random Linear Network Coding Approach to Multicast," *IEEE Trans. Inform. Theory*, vol. 52, no. 10, pp. 4413–4430, 2006.

[10] G. O. H. Katona, "Families of Subsets Having no Subset Containing Another One with Small Difference," *Nieuw Arch. Wiskd.*, vol. 20, no. 3, pp. 54–67, 1972.

[11] D. J. Kleitman, "On an Extremal Property of Antichains in Partial Orders, the LYM Property and Some of Its Implications and Applications," in: M. Hall Jr. and J. H. Van Lint (Eds.), *Combinatorics*, pp. 277–290, Amsterdam, 1975.

[12] M. Kovačević, "Runlength-Limited Sequences and Shift-Correcting Codes: Asymptotic Analysis," *IEEE Trans. Inform. Theory*, vol. 65, no. 8, pp. 4804–4814, 2019.

[13] M. Kovačević and P. Popovski, "Zero-Error Capacity of a Class of Timing Channels," *IEEE Trans. Inform. Theory*, vol. 60, no. 11, pp. 6796–6800, 2014.

[14] M. Kovačević and V. Y. F. Tan, "Codes in the Space of Multisets—Coding for Permutation Channels with Impairments," *IEEE Trans. Inform. Theory*, vol. 64, no. 7, pp. 5156–5169, 2018.

[15] M. Kovačević and D. Vukobratović, "Subset Codes for Packet Networks," *IEEE Commun. Lett.*, vol. 17, no. 4, pp. 729–732, 2013.

[16] R. Kötter and F. R. Kschischang, "Coding for Errors and Erasures in Random Network Coding," *IEEE Trans. Inform. Theory*, vol. 54, no. 8, pp. 3579–3591, 2008.

[17] A. Lenz, P. H. Siegel, A. Wachter-Zeh, and E. Yaakobi, "Coding Over Sets for DNA Storage," *IEEE Trans. Inform. Theory*, vol. 66, no. 4, pp. 2331–2351, 2020.

[18] S. Shamai (Shitz) and E. Zehavi, "Bounds on the Capacity of the Bit-Shift Magnetic Recording Channel," *IEEE Trans. Inform. Theory*, vol. 37, no. 3, pp. 863–872, 1991.

[19] E. Sperner, "Ein Satz über Untermengen einer endlichen Menge," *Math. Z.*, vol. 27, pp. 44–48, 1928.

[20] R. P. Stanley, *Enumerative Combinatorics*, Vol I, Cambridge University Press, 1997.

[21] J. H. van Lint and R. M. Wilson, *A Course in Combinatorics*, 2nd ed., Cambridge University Press, 2001.