Decoding in Weighted Combinatorial Metrics

Vladimir R. Sidorenko, Christian Senger, Martin Bossert
Inst. of Telecommunications and Applied Information Theory
Ulm University, Ulm, Germany,
{vladimir.sidorenko | christian.senger | martin.bossert}@uni-ulm.de

Abstract

Many metrics used in coding theory are instances of a combinatorial metric introduced by Gabidulin. We define a *weighted* combinatorial quasimetric. Some relations between these two metrics are established. Given an error and erasure decoder for the combinatorial metric, we propose the Forney-Kovalev soft-input-decoder for the weighted combinatorial metric. The error correcting radius of the algorithm is obtained for given number of decoding trials.

I. Introduction

Many metrics used in coding theory, including Hamming metric, burst metric [1], array metric [2], translational metrics [3], [4], and others, are particular cases of the wide class of combinatorial metrics introduced in [1] by Gabidulin. Hence, results obtained for combinatorial metrics are general and can find many applications in coding theory. Combinatorial metrics fit well to describe channels with memory.

For some combinatorial metrics, error correcting codes were proposed. Thousands of publications can be found about codes for the Hamming metric, the most popular metric in coding theory. There are codes for the burst metric, for the array metric [2], [5], for translational metrics [4], and others. In [2], [4], [5] it was shown that codes having distance d in the array metric or in translational metrics (which include e.g. burst metrics) can be obtained by a special interleaving of codes having distance d in the Hamming metric. This allows to use for these combinatorial metrics powerful algebraic decoders designed for the Hamming metric correcting up to $d/2$ and even more errors. We recall the definition of combinatorial metrics in Section II.

Frequently the communication channel gives us reliabilities (real numbers h_m) for positions in the received word. We use these reliabilities as weights to define weighted combinatorial metrics. This should be done in a way such that the weighted combinatorial metric matches the communication channel. In this case the maximum likelihood decoding coincides (exactly or approximately) with the minimum distance decoding in the weighted combinatorial metric. This approach was used for the Hamming metric by Forney [6], and for the array metric in [5]. In this paper we introduce weighted combinatorial metrics in general.

A. Decoding in weighted Hamming metric.

For the h-weighted Hamming distance $d_h(\cdot,\cdot)$, where h is a vector of reliabilities, Forney [6] suggested generalized minimum distance (GMD) decoder based on an error and erasure decoder $\Phi(\lambda)$ for the Hamming metric. The decoder $\Phi(\lambda)$ corrects ε errors and θ erasures if $\lambda\varepsilon + \theta \leq d-1$, where $\lambda = 2$ is the tradeoff rate between errors and erasures for the decoder, and d is the Hamming distance of the code. The *idea of GMD decoding* is as follows. For $j = 1, \ldots, s$ we make a trial to decode the received vector y in which the τ_j least reliable symbols are erased. Performing s decoding trials we obtain a list $\mathcal{L}$ of codewords. If this list is empty, we declare a decoding failure, otherwise we select from the list a codeword c that minimizes $d_h(c, y)$. GMD decoders may differ by using different decoders $\Phi(\lambda)$ or by different number s of decoding trials or by different selection of the erasure vector $\tau = (\tau_1, \ldots, \tau_s)$.

This work of V.R. Sidorenko has been supported by DFG (German Research Council) under grant BO 867/21. V.R. Sidorenko is on leave from Kharkevich Institute for Information Transmission Problems, Russian Academy of Sciences, Moscow, Russia.

In [6] Forney considered GMD decoder with $s = \lceil d/2 \rceil$ decoding trials and show that its error correcting radius in weighted Hamming metric is $\rho = d$. In his algorithm, the erasing vector τ does not depend on the vector of reliabilities h. Hence, the vector τ is fixed for fixed d.

In [7] Kovalev considered GMD decoding algorithms for the cases when the number of trials s can be less then $\lceil d/2 \rceil$, i.e., $1 \leq s \leq \lceil d/2 \rceil$. In addition, Kovalev considered two strategies: fixed erasing, when the vector τ does not depend on h, and adaptive erasing, when τ is optimized using the vector of reliabilities h.

Some refinements of Kovalev's approaches were done by Weber and Abdel-Ghaffar in [8]. We should also mention papers by Sorger [9], and Kötter [10] who suggested interesting modifications of a BMD decoder in such a way that multi–trial decoding can be done "in one step". We do not consider other interesting erasing strategies suggested by Blokh and Zyablov [11] based on reliability thresholds. This could be a topic for additional research. There are many interesting publications concerning GMD decoding in Hamming metric using bounded minimum distance decoders, $\lambda = 2$, see e.g. Dumer [12] and Kabatyanskii [13]. For $\lambda < 2$ the Forney-Kovalev algorithm was extended in [14] and [15] using decoders $\Phi(\lambda)$ from [16] and [17].

B. Our contribution

For the weighted *array* metrics the Forney-Kovalev (FK) algorithm was extended in [5]. In this paper we extend the FK algorithm to the *arbitrary* weighted combinatorial metric. In Section III we define weighted combinatorial metrics and obtain some useful properties of the metrics. In Section IV we describe the FK algorithm and give an important Lemma 5 where error correcting radius $\delta(\tau, h)$ for fixed reliability vector h and fixed erasing strategy τ is calculated. After $\delta(\tau, h)$ is obtained we apply results from [14] to estimate the error correction radius of the FK algorithm in general case. This was done in Section V, where the simplified version of the FK decoder is shown by Algorithm 1.

II. Combinatorial metrics and codes

A. Combinatorial metrics

Consider an arbitrary alphabet Q and words of length N over this alphabet. Given two words $a, b \in Q^N$, denote by $\{a \neq b\}$ the *difference set*, i.e., the set of positions in which a and b do not coincide:

$$\{a \neq b\} \triangleq \{n \in [1, N] : a_n \neq b_n\}. \tag{1}$$

Consider a set $T = \{T_1, \ldots, T_M\}$ of M basis sets $T_m \subseteq [1, N]$, $m = 1, \ldots, M$, such that $\bigcup T_m = [1, N]$. Given a set $A \subseteq [1, N]$, denote by $I_A \subseteq [1, M]$ a set of indexes such that the basis sets with these indexes cover the set A, i.e., $A \subseteq \bigcup_{m \in I_A} T_m$.

Definition 1 *The combinatorial T-distance $d(a, b)$ between two words $a, b \in Q^N$ is the minimum number of basis sets T_m that cover the difference set $\{a \neq b\}$, i.e.,*

$$d(a, b) = \min_{I_{\{a \neq b\}}} |I_{\{a \neq b\}}|. \tag{2}$$

The combinatorial distance was suggested in [1], where it was shown that it satisfies the axioms of a metric.

B. Error and erasure correcting codes

A *code* C is a subset of Q^N, $C \subseteq Q^N$. Given a T-combinatorial metric, the *code distance* $d(C)$ in this metric is the minimum distance between two different codewords. If a codeword $c \in C$ was transmitted and a word $y \in Q^N$ was received, we say that it was an *error of weight* $\varepsilon = d(x, y)$ in the channel. Given a received word y, the *minimum distance decoder* finds a codeword c nearest to y, i.e., it finds $c \in C$

such that $d(c,y)$ is minimal. The minimum distance decoder is able to correct every error of weight less than $d/2$.

Erasures. Assume that the channel informs us that some positions in the received word y are absolutely unreliable. This means that symbols at these positions in y are unknown (erased). More precisely, the channel gives us the received word y and a set $X \subseteq [1,M]$ of the minimum cardinality such that the positions in y that belong to $\bigcup_{m\in X} T_m$ are erased. We say that the weight of the erasure is $\theta = |X|$. Let us find a set $I \subseteq [1,M]$ of the minimum cardinality such that $\{c \neq y\} \subseteq \bigcup_{m\in X\cup I} T_m$. Then the error weight ε on unerased positions is $\varepsilon = |I|$.

For many combinatorial metrics there are codes and error and erasure decoders $\Phi(\lambda)$ correcting (for sure or with very high probability) an error of weight ε and an erasure of weight θ as soon as

$$\lambda\varepsilon + \theta \leq d(C) - 1, \tag{3}$$

where $1 < \lambda \leq 2$ is the tradeoff rate between errors and erasures for the particular decoder.

III. Weighted combinatorial metrics and decoding

A. Weighted combinatorial metrics

Given a vector $h = (h_1, \ldots, h_M)$, where $0 \leq h_m \leq 1$, we define weighted T-distance as follows.

Definition 2 *Given a T-metric and a vector h, the weighted combinatorial h-distance $d_h(a,b)$ between words $a, b \in Q^N$ is defined as follows*

$$d_h(a,b) = \min_{I_{\{a\neq b\}}} \left(\sum_{m\in I_{\{a\neq b\}}} (1+h_m) + \sum_{m\notin I_{\{a\neq b\}}} (1-h_m) \right). \tag{4}$$

The weight h_m can be seen as a reliability of positions in the received word y that belong to the basis set T_m. The more h_m the more reliable these positions are. If $h_m = 0$ then these positions are erased.

Theorem 1 *The h-distance in Definition 2 satisfies the axioms of a quasinorm, i.e., for every $a, b, c \in Q^N$*

1) $d_h(a,b) \geq 0$,
2) $d_h(a,b) = d_h(b,a)$,
3) $d_h(a,b) \leq d_h(a,c) + d_h(c,b)$.

Notice that the h-distance does not satisfy the axiom of identity of indiscernibles: $d_h(a,b) = 0$ if and only if $a = b$.

Denote by $d_h(C)$ the code distance of the code C in the weighted combinatorial h-distance. The following theorems give us some relations between combinatorial and a weighted combinatorial distances.

Lemma 2 *For all weight vectors h and for all $a, b \in Q^N$ hold*

$$d_h(a,b) \geq d(a,b), \quad \textit{and} \quad \min_h d_h(a,b) = d(a,b), \tag{5}$$

$$d_h(C) \geq d(C), \quad \textit{and} \quad \min_h d_h(C) = d(C). \tag{6}$$

For $h = (1,1,\ldots,1)$ holds

$$d_h(a,b) = 2d(a,b). \tag{7}$$

Lemma 3 *For all weight vectors h and for all $y, c, \tilde{c} \in Q^N$ such that $d(\tilde{c}, c) \geq d$ holds*

$$d_h(c,y) + d_h(\tilde{c},y) \geq 2d. \tag{8}$$

B. Decoders in weighted combinatorial metric

Given a received word y and reliability vector h, the *g*oal of the h-distance decoder is to find the codeword c at the minimum h-distance $d_h(y,c)$ from y, i.e., to decode the code C in the h-metric.

The guaranteed error correcting radius ρ of a particular decoder is the infimum of real numbers $\tilde{\rho}$, for which there exist two words $c \in C$, $y \in Q^N$ and a vector $h \in [0,1]^M$, such that $d_h(y,c) = \tilde{\rho}$, and the decoder fails to decode y, h, i.e., the decoder does not output c. In other words, we guarantee correction of every error of h-weight less than ρ, where the error-weight is defined to be $d_h(y,c)$.

It follows from Lemma 2 that the error-correcting radius ρ of any decoder in h-metric can not be greater than d. From Lemma 3 we get the following

Theorem 4 *For arbitrary received word y and vector h, at most one codeword c satisfies $d_h(y,c) < d(C)$.*

IV. Forney-Kovalev (FK) decoding

To implement decoding in a combinatorial h-metric we use the FK algorithm. Given an error-and-erasure decoder $\Phi(\lambda)$ of the code C in the combinatorial metric, the *FK decoding* is as follows. For $j = 1, \ldots, s$ we make a trial to decode the received word y in which the τ_j least reliable sets of positions are erased. Performing s decoding trials using decoder $\Phi(\lambda)$ we obtain a list $\mathcal{L}$ of codewords. If this list is empty, we declare a decoding failure, otherwise we output a codeword c having the minimum $d_h(c,y)$. This codeword is unique due to Theorem 4 if the h-weight of error in the channel is less than $d(C)$.

FK decoders may differ by using different decoders $\Phi(\lambda)$ (having different λ) or by different number s of decoding trials or by different selection of the erasure vector $\tau = (\tau_1, \ldots, \tau_s)$. If $s = \lceil d(C)/2 \rceil$ and the erasure vector is fixed we get the Forney algorithm. If $s < \lceil d(C)/2 \rceil$ or the erasure vector is selected adaptive depending on the received vector h of reliabilities, we obtain the Kovalev algorithm, having better error correcting radius. Later we consider the adaptive approach only.

Let us estimate the guaranteed error correcting radius ρ of the adaptive FK algorithm. Recall that we consider a FK decoder based on an error-and-erasure correcting decoder $\Phi(\lambda)$ which satisfies (3) with tradeoff rate λ. At the input of the FK decoder we have a received word y and a vector of reliabilities h. From now on, assume w.l.o.g. that the bases sets T_m are numbered according to their reliabilities as follows

$$0 \le h_1 \le h_2 \le \cdots \le h_M \le 1. \tag{9}$$

So, we denote by $h = (h_1, ..., h_M)$ the vector of *ordered* reliabilities, and by $\mathcal{H}$ the set of all possible real-valued vectors h satisfying (9).

Definition 3 *Given the vector h of reliabilities, by $\delta_\tau(h)$ we denote the minimum h-weight of the error in the channel that causes a failure of the FK decoder with erasing strategy defined by the vector τ. In other words, $\delta_\tau(h)$ is error-correcting radius for fixed h and τ.*

Lemma 5 *Error-correcting radius $\delta_\tau(h)$ is as follows*

$$\delta_\tau(h) = \sum_{m=1}^{M} (1 - h_m) + 2 \sum_{j=1}^{s} \sum_{m=\tau_j+1}^{\tau_j+\varepsilon(\tau_j)-\varepsilon(\tau_{j+1})} h_m, \tag{10}$$

where we denote the function

$$\varepsilon(\theta) = \left\lfloor \frac{d - \theta - 1}{\lambda} \right\rfloor + 1,$$

and τ_{s+1} is formally defined such that $\varepsilon(\tau_{s+1}) = 0$.

Let $\mathcal{T}$ be the set of all integer-valued vectors $\tau = (\tau_1, ..., \tau_s)$ such that $0 \le \tau_1 \le \cdots \le \tau_s \le d-1$. To specify a particular FK decoder we are free to select a vector τ. For a given h we will select τ to maximize the error-correcting radius $\delta_\tau(h)$:

$$\tau(h) = \arg\max_{\tau \in \mathcal{T}} \delta_\tau(h). \tag{11}$$

The algorithm with this $\tau(h)$ we call the *adaptive algorithm* and denote by A. The error correcting radius $\rho_A(\lambda)$ of algorithm A is

$$\rho_A(\lambda) = \inf_{h \in \mathcal{H}} \max_{\tau \in \mathcal{T}} \delta_\tau(h). \tag{12}$$

To find vector $\tau(h)$ from (11) one should consider $|\mathcal{T}|$ vectors τ, thus the complexity of this step is $\mathcal{O}(d^s)$. Remark, that the decoder should compute $\tau(h)$ for every received h, thus the computation is only feasible for one or two decoding trials, i.e., for $s = 1, 2$. This is a big disadvantage of the adaptive approach using the erasing vector (11).

V. Error correction radii

Fortunately Kovalev suggested a simplification of the adaptive decoding algorithm where vector of erasures $\tau(h)$ should be selected from a set of two vectors only! In [14] this simplified algorithm was extended for all the range of λ and the final decoder is given by Algorithm 1. To compute $\tau(h)$, Algorithm 1 requires $\mathcal{O}(d)$ operations only. Error-correcting radius $\rho_A(\lambda)$ of the initial algorithm A based on $\tau(h)$ given by (11) and radius of the simplified Algorithm 1 coincide!

Algorithm 1: Simplified s-trial adaptive decoding

Precomputations: Solve (14), get vectors $\tau^{(a)} = (\tau_0, \tau_2, ..., \tau_{2(s-1)})$ and $\tau^{(b)} = (\tau_1, \tau_3, ..., \tau_{2s-1})$;
Input: received word y and (ordered) vector h;
Select vector $\tau' = \arg\max_{\tau \in \{\tau_a, \tau_b\}} \delta_\tau(h)$;
for *each* j *from* 1 *to* s **do**
  decode y with erased first τ'_j sets T_m by the decoder $\Phi(\lambda)$ of the code C, add obtained codeword (if any) to the list $\mathcal{L}$;
Output:
if *the list* $\mathcal{L}$ *is empty* **then**
  declare a decoding failure;
else
  output $c \in \mathcal{L}$ having minimum $d_h(c, y)$

Theorem 6 ([14]) *The guaranteed error correcting radius of Algorithm 1 is lower bounded by* $\underline{\rho}_A(\lambda)$

$$\rho_A(\lambda) \ge \underline{\rho}_A(\lambda) = \varepsilon(0) + \varepsilon(\tau_1), \tag{13}$$

where τ_1 *is a solution of recurrent inequalities*

$$\tau_i \ge \tau_{i-1} + \varepsilon(\tau_{i-1}) - \varepsilon(\tau_{i+1}), \quad i = 1, \ldots, 2s-1, \tag{14}$$

with boundary conditions

$$\tau_0 = 0, \quad \tau_{2s} = \lfloor d - 1 + \lambda \rfloor. \tag{15}$$

The lower bound (13) is nearly tight [14] and can be approximated as follows.

Corollary 7 *For $1 < \lambda < 2$ the s-trial guaranteed error correcting radius of Algorithm 1 is lower bounded by*

$$\underline{\rho}_A(\lambda) \approx d\left(1 - \frac{(2-\lambda)(\lambda-1)^{2s}}{\lambda(1-(\lambda-1)^{2s})}\right) \approx d\left(1-(\lambda-1)^{2s}\right). \tag{16}$$

To reach $\rho_A(\lambda) = d$ it is sufficient to have $s = \frac{1}{2}\left(\log_{\frac{1}{\lambda-1}} d + 1\right)$ decoding trials.

Corollary 8 *For $\lambda = 2$ the s-trial guaranteed error correcting radius of Algorithm 1 is lower bounded by*

$$\underline{\rho}_A(2) = d + 1 - \left\lceil \frac{d+1}{4s} \right\rceil, \tag{17}$$

which coincides with Kovalev's result in case of the Hamming metric. To reach $\underline{\rho}_A(2) = d$ it is sufficient to have $s = \left\lceil \frac{d+1}{4} \right\rceil$ decoding trials.

Notice, to reach $\underline{\rho}_A(\lambda) = d$, the number s of decoding trials grows linearly with d for the classical case $\lambda = 2$ and only logarithmically for $\lambda < 2$. As a result, for $\lambda < 2$ the error-correcting radius of Algorithm 1 quickly approaches d with increasing number of trials, and 2 or 3 trials are sufficient to reach $\rho_A(\lambda) = d$ in many practical cases.

It is interesting to remark that we can reach the error correcting radius $\rho = d$ despite $\min_h(C) = d$ according to Lemma 2.

REFERENCES

[1] E. M. Gabidulin, "Combinatorial metrics in coding theory," *2nd Int. Symp. on Inf. Theory*, Budapest Akadimiai Kaido, 169-176, 1973.

[2] E.M. Gabidulin, B.I. Korjik, "Lattice-error-correcting codes," *Izv. Vyssh. Uchebn. Zaved., Radioelektron.*, 15, no. 4, 492-498, 1972.

[3] E. Gabidulin, "Metrics in Coding Theory," *Multiple Access Channels, Theory and Practice*, Vol. 10 NATO Security through Science Series: Information and Communication Security Editors: E. Biglieri and L. Gyrfi April 2007, 360, ISBN: 978-1-58603-728-4.

[4] V. Sidorenko, "Tilings of the Plane and Codes for Translational Combinatorial Metrics," *IEEE Int. Symp. on Inf. Theory,* Trondheim, Norway, p. 107, 1994.

[5] V. Sidorenko, M. Bossert, E. Gabidulin, "Generalized Minimum Distance Decoding for Correcting Array Errors," *Int. Zurich Seminar on Communications (IZS)*, 102-105, March 3-5, 2010.

[6] G. D. Forney Jr., "Generalized minimum distance decoding," *IEEE Trans. Inf. Theory*, vol. 12, pp. 125-131, Apr. 1966.

[7] S. I. Kovalev, "Two classes of minimum generalized distance decoding algorithms," *Probl. Pered. Inform.*, vol. 22, no. 3, 35-42, 1986.

[8] J. H. Weber, K. A. S. Abdel-Ghaffar, "Reduced GMD decoding," *IEEE Trans. Inf. Theory*, vol. 49, pp. 1013-1027, April 2003.

[9] U. K. Sorger, "A new Reed-Solomon code decoding algorithm based on Newton's interpolation," *IEEE Trans. Inf. Theory*, vol. 39, no. 2, pp. 358-365, 1993.

[10] R. Kötter, "Fast generalized minimum-distance decoding of Algebraic-Geometry and Reed-Solomon codes," *IEEE Trans. Inf. Theory*, vol. 42, no. 3, pp. 721-737, May 1993.

[11] E. L. Blokh and V. V. Zyablov, Linear Concatenated Codes. Nauka, 1982. In Russian.

[12] I. I. Dumer, "Concatenated codes and their multilevel generalizations," in Handbook of Coding Theory, vol. II, ch. 23, Amsterdam: North-Holland, 1998. ISBN 0-444-50087-1.

[13] G.A. Kabatyanskii, "About metrics and decoding domains of Forney's algorithm," *Proc. 5th Joint Swedish-Soviet Workshop on Information Theory*, pp. 81–85 , 1991.

[14] V. Sidorenko, A. Chaaban, Ch. Senger, M. Bossert, "On Extended Forney-Kovalev GMD decoding," *IEEE Intern. Symposium on Inf. Theory*, June-July, 2009, Seoul, Korea.

[15] V. R. Sidorenko, C. Senger, M. Bossert, V. V. Zyablov, "Single-trial decoding of concatenated codes using fixed or adaptive erasing," *Advances in Mathematics of Communications*, Vol. 4, No. 1, 4960, Febr. 2010.

[16] V. R. Sidorenko, G. Schmidt, M. Bossert, "Decoding punctured Reed-Solomon codes up to the Singleton bound," in *Proc. of Int. ITG Conference on Source and Channel Coding*, Ulm, January 2008.

[17] G. Schmidt, V. R. Sidorenko, and M. Bossert, "Collaborative decoding of interleaved Reed–Solomon codes and concatenated code designs,"*IEEE Trans. Inf. Theory*, vol. 55, n. 7, pp. 2991-3012, July 2009.