The bound can also be adapted to continuous alphabets by replacing the probability distribution $p(\cdot)$ by a density, the cardinality $|B_n(\rho)|$ by a volume, and the entropy $H(p)$ by the corresponding differential entropy. With these substitutions—and provided that a density $p(\cdot)$ of the form (3) and satisfying (4) exists—the nonasymptotic part of the first proof, and thus the bound (2), is still valid. We conclude with the following example due to G. D. Forney, Jr., (private communication).

Example: Let A be the real line with weight $w(a) = a^2$; then $B_n(\rho)$ is the n-dimensional sphere (ball) of radius $\sqrt{n\rho}$ around the origin. The probability density $p(\cdot)$ is Gaussian with variance ρ, whose differential entropy is $\log_2 \sqrt{2\pi e \rho}$. According to (the continuous version of) (2), the volume of $B_n(\rho)$ is upper bounded by $(2\pi e \rho)^{n/2}$. The comparison of this bound, for $n = 2m$, with the exact formula $(2m\rho\pi)^m/m!$ for the volume yields the Stirling-type bound

$$m! \geq (m/e)^m,$$

derived purely from information theory and geometry. (The Stirling approximation is $m! \approx \sqrt{2\pi m}(m/e)^m$.)

APPENDIX
PROOF OF THE PROPOSITION

To simplify notation, we write w_i and p_i instead of $w(a_i)$ and $p(a_i)$, respectively. All logarithms are to the base 2.

We assume, without loss of essential generality, that $w_1, \cdots, w_m$ are the elements of A that have minimal weight. For $\lambda = 0$, $p(\cdot)$ is uniform over A, and thus $E[w] = \bar{w}$ and $H(p) = \log|A|$. The limits as $\lambda \to \infty$ of $p(\cdot)$ is the distribution $p_i = 1/m$ for $1 \leq i \leq m$ and $p_i = 0$ otherwise, which makes it clear that $\lim_{\lambda\to\infty} E[w] = w_{\min}$ and $\lim_{\lambda\to\infty} H(p) = \log m$.

We next show that $(d/d\lambda)E[w] < 0$ for all λ. Let $f(\lambda) \triangleq \sum_i w_i e^{-\lambda w_i}$.

$$\begin{aligned}
&[\mathcal{Z}(\lambda)]^2 \frac{d}{d\lambda} E[w] \\
&\quad = [\mathcal{Z}(\lambda)]^2 \frac{d}{d\lambda}[f(\lambda)/\mathcal{Z}(\lambda)] \\
&\quad = \mathcal{Z}(\lambda)\frac{d}{d\lambda} f(\lambda) - f(\lambda)\frac{d}{d\lambda}\mathcal{Z}(\lambda) \\
&\quad = -\sum_i e^{-\lambda w_i}\sum_j w_j^2 e^{-\lambda w_j} + \sum_i w_i e^{-\lambda w_i}\sum_j w_j e^{-\lambda w_j} \\
&\quad = -\sum_i \sum_j e^{-\lambda(w_i+w_j)} w_j(w_j - w_i) \\
&\quad = -\sum_i \sum_{j>i} e^{-\lambda(w_i+w_j)}[w_j(w_j - w_i) + w_i(w_i - w_j)] \\
&\quad = -\sum_i \sum_{j>i} e^{-\lambda(w_i+w_j)}(w_i - w_j)^2,
\end{aligned}$$

which is negative unless all weights are equal. Since $\mathcal{Z}(\lambda) > 0$, we have proved that $(d/d\lambda)E[w] < 0$ for all λ.

The monotonic decrease of $H(p)$ follows from the relation $(d/d\lambda)H(p) = \lambda \log e\,(d/d\lambda)E[w]$, which results from the following calculation:

$$\begin{aligned}
\frac{d}{d\lambda} H(p) &= \sum_i \frac{\partial}{\partial p_i} H(p)\frac{dp_i}{d\lambda} \\
&= -\sum_i \frac{\partial}{\partial p_i}(p_i \log p_i)\frac{dp_i}{d\lambda} \\
&= -\sum_i (\log p_i + \log e)\frac{dp_i}{d\lambda} \\
&= \sum_i (\lambda w_i \log e + \log \mathcal{Z}(\lambda) - \log e)\frac{dp_i}{d\lambda} \\
&= \lambda \log e \sum_i w_i \frac{dp_i}{d\lambda} \\
&= \lambda \log e \sum_i \frac{\partial}{\partial p_i}(p_i w_i)\frac{dp_i}{d\lambda} \\
&= \lambda \log e \frac{d}{d\lambda} E[w].
\end{aligned}$$

ACKNOWLEDGMENT

This note benefitted greatly from detailed comments by J. L. Massey, F. R. Kschischang, G. D. Forney, Jr., and T. Ericson.

REFERENCES

[1] F. J. McWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes.* Amsterdam: Elsevier, 1988.

[2] Ph. Piret, "Bounds for codes over the unit circle," *IEEE Trans. Inform. Theory*, vol. IT-32, pp. 760–767, Nov. 1986.

[3] G. D. Forney, Jr. and L.-F. Wei, "Multidimensional constellations—Part I: Introduction, figures of merit, and generalized cross constellations," *IEEE J. Select. Areas Commun.*, vol. 7, pp. 877–892, Aug. 1989.

[4] T. M. Cover and J. A. Thomas, *Elements of Information Theory.* New York: Wiley, 1991.

[5] E. Schrödinger, *Statistical Mechanics.* Cambridge: Cambridge Univ. Press, 1962.

[6] J. M. Wozencraft and I. M. Jacobs, *Principles of Communication Engineering.* New York: Wiley, 1965.

Asymptotic Results on Codes for Symmetric, Unidirectional, and Asymmetric Error Control

Jos H. Weber

***Abstract*—The asymptotic behavior of the rates of optimal codes correcting and/or detecting combinations of symmetric, unidirectional, and/or asymmetric errors is studied. These rates are expressed in terms of the rate of optimal codes with a certain Hamming distance. As a consequence, well-known bounds on the latter rate can also be applied to bound the former rates. Furthermore, it turns out that, without losing rate asymptotically, any error control combination can be upgraded to simultaneous symmetric error correction/detection and all unidirectional error detection.**

***Index Terms*—Asymmetric errors, code rate, error correction, error detection, symmetric errors, unidirectional errors.**

I. INTRODUCTION

We consider binary channels over which codewords from a block code $\mathcal{C}$ are sent. If a received word differs in e coordinates from the transmitted word, we say that e (symmetric) errors have occurred. If these transitions are all of the same type (either 1 → 0 or 0 → 1), the error pattern is said to be unidirectional, while if all transitions are of the 1 → 0 type, the error pattern is said to be asymmetric. So any asymmetric error pattern is also unidirectional, and any unidirectional error pattern is also symmetric. We call e the weight of the error pattern.

Manuscript received December 23, 1993; revised May 9, 1994. This paper was presented at the 15th Symposium on Information Theory in the Benelux, Louvain-la-Neuve, Belgium, May 1994.

IEEE Log Number 9406221.

The author is with the Department of Electrical Engineering, Delft University of Technology, 2600 GA Delft, The Netherlands.

We call a code t_1-SyEC t_2-UEC t_3-AsEC d_1-SyED d_2-UED d_3-AsED (with $t_1 \le t_2 \le t_3$, $d_1 \le d_2 \le d_3$, $0 \le t_i \le d_i$) if and only if it can simultaneously correct up to t_1 symmetric errors, up to t_2 unidirectional errors, and up to t_3 asymmetric errors, as well as detect more than t_1 up to d_1 symmetric errors that are not of the unidirectional type, more than t_2 up to d_2 unidirectional errors that are not of the asymmetric type, and more than t_3 up to d_3 asymmetric errors. Hence, for an error pattern of weight e, the control capabilities of such codes are as follows. In case all errors are of the $1 \to 0$ type, the errors are corrected if $e \le t_3$ and detected if $t_3 < e \le d_3$. In case all errors are of the $0 \to 1$ type, the errors are corrected if $e \le t_2$ and detected if $t_2 < e \le d_2$. Finally, in case the errors are of a mixed type, the errors are corrected if $e \le t_1$ and detected if $t_1 < e \le d_1$.

A necessary and sufficient condition for a code to have the property described above is given in the next theorem. For a proof, we refer to [2]. For two vectors $\boldsymbol{x}$ and $\boldsymbol{y}$ of equal length, we define $N(\boldsymbol{x}, \boldsymbol{y}) = |\{i : x_i = 0 \wedge y_i = 1\}|$, while $D(\boldsymbol{x}, \boldsymbol{y})$ denotes the Hamming distance between $\boldsymbol{x}$ and $\boldsymbol{y}$, i.e., $D(\boldsymbol{x}, \boldsymbol{y}) = N(\boldsymbol{x}, \boldsymbol{y}) + N(\boldsymbol{y}, \boldsymbol{x})$.

Theorem 1 [2]: A code $\mathscr{C}$ is t_1-SyEC t_2-UEC t_3-AsEC d_1-SyED d_2-UED d_3-AsED (with $t_1 \le t_2 \le t_3$, $d_1 \le d_2 \le d_3$, $0 \le t_i \le d_i$) if and only if all $\boldsymbol{x}, \boldsymbol{y} \in \mathscr{C}$ with $\boldsymbol{x} \ne \boldsymbol{y}$ and $N(\boldsymbol{x}, \boldsymbol{y}) \ge N(\boldsymbol{y}, \boldsymbol{x})$ satisfy

$$\begin{cases} D(\boldsymbol{x}, \boldsymbol{y}) \ge t_2 + d_3 + 1 & \\ \quad \wedge D(\boldsymbol{x}, \boldsymbol{y}) \ge t_3 + d_2 + 1 & \text{if } N(\boldsymbol{y}, \boldsymbol{x}) = 0, \\ D(\boldsymbol{x}, \boldsymbol{y}) \ge t_1 + d_3 + 1 & \\ \quad \wedge D(\boldsymbol{x}, \boldsymbol{y}) \ge t_3 + d_1 + 1 & \\ \quad \wedge N(\boldsymbol{x}, \boldsymbol{y}) \ge d_3 + 1 & \text{if } 1 \le N(\boldsymbol{y}, \boldsymbol{x}) \le t_3, \\ D(\boldsymbol{x}, \boldsymbol{y}) \ge t_3 + d_1 + 1 & \text{if } N(\boldsymbol{y}, \boldsymbol{x}) \ge t_3 + 1. \end{cases}$$

□

Many well-known conditions can be derived as special cases of this general result by choosing appropriate error control parameters t_i and d_i. For example, substituting $t_1 = t_2 = t_3 = d_1 = t$ and $d_2 = d_3 = d$ gives the necessary and sufficient condition for a code to be t-SyEC d-UED. If we want all unidirectional errors to be detected, then we choose d equal to the length of the code, and the resulting code is t-SyEC AUED (all unidirectional error detecting).

Let $M(n, t_1, t_2, t_3, d_1, d_2, d_3)$ be defined as the maximum number of codewords in a t_1-SyEC t_2-UEC t_3-AsEC d_1-SyED d_2-UED d_3-AsED code of length n. Hence, the maximum attainable rate of such a code equals

$$\frac{\log_2 M(n, t_1, t_2, t_3, d_1, d_2, d_3)}{n}. \tag{1}$$

In the next section, we study the asymptotic behavior of this rate.

II. ASYMPTOTIC RESULTS

As usual in coding theory, let $A(n, d)$ denote the maximum number of codewords in a code of length n in which any two different codewords are at least Hamming distance d apart. Hence, the maximum attainable rate of such a code equals

$$\frac{\log_2 A(n, d)}{n}. \tag{2}$$

When studying the asymptotic behavior of (2), it is convenient to define

$$\alpha(\delta) = \limsup_{n \to \infty} \frac{\log_2 A(n, n\delta)}{n} \tag{3}$$

for $\delta \ge 0$.

In order to study the asymptotic behavior of (1), we now similarly define

$$\mu(\tau_1, \tau_2, \tau_3, \delta_1, \delta_2, \delta_3) = \limsup_{n \to \infty} \frac{\log_2 M(n, n\tau_1, n\tau_2, n\tau_3, n\delta_1, n\delta_2, n\delta_3)}{n} \tag{4}$$

for $\tau_1 \le \tau_2 \le \tau_3$, $\delta_1 \le \delta_2 \le \delta_3$, $0 \le \tau_i \le \delta_i \le 1$. Hence, we fix the ratios between the error control parameters and the length, and consider the rate when n is large. Next, we derive two lemmas, which are useful in evaluating (4).

Lemma 2: For $t_1 \le t_2 \le t_3$, $d_1 \le d_2 \le d_3$, $0 \le t_i \le d_i \le n$, we have

$$M(n, t_1, t_2, t_3, d_1, d_2, d_3) \le (n+1) A(n, t_3 + \max\{t_3 + 1, d_1\} + 1).$$

Proof: Let $\mathscr{C}$ be a t_1-SyEC t_2-UEC t_3-AsEC d_1-SyED d_2-UED d_3-AsED code of length n and size $M(n, t_1, t_2, t_3, d_1, d_2, d_3)$. Let $\mathscr{C}_w$ denote all codewords in $\mathscr{C}$ of weight w. Let $\boldsymbol{x}$ and $\boldsymbol{y}$ be any two different codewords in $\mathscr{C}_w$. Suppose $N(\boldsymbol{y}, \boldsymbol{x}) \le t_3$; then either $N(\boldsymbol{x}, \boldsymbol{y}) = N(\boldsymbol{y}, \boldsymbol{x}) = 0$, which would imply $\boldsymbol{x} = \boldsymbol{y}$, or $1 \le N(\boldsymbol{x}, \boldsymbol{y}) = N(\boldsymbol{y}, \boldsymbol{x}) \le t_3$, which would imply $d_3 + 1 \le N(\boldsymbol{x}, \boldsymbol{y}) \le t_3$ by Theorem 1. Because of these contradictions, we have $N(\boldsymbol{x}, \boldsymbol{y}) = N(\boldsymbol{y}, \boldsymbol{x}) \ge t_3 + 1$, and thus by Theorem 1, it follows that $D(\boldsymbol{x}, \boldsymbol{y}) \ge \max\{t_3 + d_1 + 1, 2(t_3 + 1)\}$. Hence,

$$\begin{aligned} M(n, t_1, t_2, t_3, d_1, d_2, d_3) &= |\mathscr{C}| = \sum_{w=0}^{n} |\mathscr{C}_w| \\ &\le (n+1) A(n, t_3 + \max\{t_3 + 1, d_1\} + 1). \end{aligned}$$

□

Lemma 3: For $t_1 \le t_2 \le t_3$, $d_1 \le d_2 \le d_3$, $0 \le t_i \le d_i \le n$, we have

$$M(n, t_1, t_2, t_3, d_1, d_2, d_3) \ge \frac{A(n, t_3 + \max\{t_3 + 1, d_1\} + 1)}{n+1}.$$

Proof: Let $\mathscr{C}$ be a code of length n, size $A(n, t_3 + \max\{t_3 + 1, d_1\} + 1)$, and Hamming distance at least $t_3 + \max\{t_3 + 1, d_1\} + 1$. Let $\mathscr{C}_w$ denote all codewords in $\mathscr{C}$ of weight w. For any two different $\boldsymbol{x}, \boldsymbol{y} \in \mathscr{C}_w$, we have $N(\boldsymbol{x}, \boldsymbol{y}) = N(\boldsymbol{y}, \boldsymbol{x}) = D(\boldsymbol{x}, \boldsymbol{y})/2 \ge t_3 + 1$ and $D(\boldsymbol{x}, \boldsymbol{y}) \ge t_3 + d_1 + 1$. By Theorem 1, $\mathscr{C}_w$ is t_1-SyEC t_2-UEC t_3-AsEC d_1-SyED d_2-UED d_3-AsED, and so

$$\begin{aligned} A(n, t_3 + \max\{t_3 + 1, d_1\} + 1) &= |\mathscr{C}| = \sum_{w=0}^{n} |\mathscr{C}_w| \\ &\le (n+1) M(n, t_1, t_2, t_3, d_1, d_2, d_3). \end{aligned}$$

□

By applying Lemmas 2 and 3 to (4), we easily obtain the following theorem.

Theorem 4: For $\tau_1 \le \tau_2 \le \tau_3$, $\delta_1 \le \delta_2 \le \delta_3$, $0 \le \tau_i \le \delta_i \le 1$, we have

$$\mu(\tau_1, \tau_2, \tau_3, \delta_1, \delta_2, \delta_3) = \limsup_{n \to \infty} \frac{\log_2 A(n, n\tau_3 + \max\{n\tau_3 + 1, n\delta_1\} + 1)}{n}.$$

□

By taking into consideration that $A(n, d)$ is nonincreasing in d, we can further evaluate the result from Theorem 4. On one hand, we have,

$$\begin{aligned} \mu(\tau_1, \tau_2, \tau_3, \delta_1, \delta_2, \delta_3) &= \limsup_{n \to \infty} \frac{\log_2 A(n, n\tau_3 + \max\{n\tau_3 + 1, n\delta_1\} + 1)}{n} \\ &\le \limsup_{n \to \infty} \frac{\log_2 A(n, n(\tau_3 + \max\{\tau_3, \delta_1\}))}{n} \\ &= \alpha(\tau_3 + \max\{\tau_3, \delta_1\}), \end{aligned} \tag{5}$$

and on the other hand, we have

$$\begin{aligned}\mu(\tau_1,\tau_2,\tau_3,\delta_1,\delta_2,\delta_3)&\\ &= \limsup_{n\to\infty}\frac{\log_2 A(n, n\tau_3+\max\{n\tau_3+1, n\delta_1\}+1)}{n}\\ &\geq \limsup_{n\to\infty}\frac{\log_2 A(n, n\tau_3+\max\{n\tau_3+n\epsilon/2, n\delta_1\}+n\epsilon/2)}{n}\\ &\geq \limsup_{n\to\infty}\frac{\log_2 A(n, n(\tau_3+\max\{\tau_3,\delta_1\}+\epsilon))}{n}\\ &= \alpha(\tau_3+\max\{\tau_3,\delta_1\}+\epsilon) \qquad (6)\end{aligned}$$

for all $\epsilon > 0$. Hence, we have the following result.

Corollary 5: For $\tau_1 \leq \tau_2 \leq \tau_3$, $\delta_1 \leq \delta_2 \leq \delta_3$, $0 \leq \tau_i \leq \delta_i \leq 1$, we have

$$\alpha(\tau_3+\max\{\tau_3,\delta_1\}) \geq \mu(\tau_1,\tau_2,\tau_3,\delta_1,\delta_2,\delta_3) \geq \lim_{\delta\to(\tau_3+\max\{\tau_3,\delta_1\})^+}\alpha(\delta).$$

□

By Corollary 5, we can easily apply well-known bounds on $\alpha(\delta)$ in order to bound $\mu(\tau_1,\tau_2,\tau_3,\delta_1,\delta_2,\delta_3)$. An overview of bounds on $\alpha(\delta)$ can be found in [1, ch. 5]. Since it is known that $\alpha(\delta) = 0$ if $\delta \geq 1/2$, we thus have

$$\mu(\tau_1,\tau_2,\tau_3,\delta_1,\delta_2,\delta_3) = 0 \qquad \text{if } \tau_3+\max\{\tau_3,\delta_1\} \geq 1/2. \tag{7}$$

If $\tau_3+\max\{\tau_3,\delta_1\} < 1/2$, then we can bound $\mu(\tau_1,\tau_2,\tau_3,\delta_1,\delta_2,\delta_3)$ by taking the best known lower and upper bounds on $\alpha(\delta)$, i.e., the Gilbert–Varshamov bound and the McEliece–Rodemich–Rumsey–Welch bound, respectively, both at $\delta = \tau_3 + \max\{\tau_3, \delta_1\}$.

By observing from Theorem 4 that $\mu(\tau_1,\tau_2,\tau_3,\delta_1,\delta_2,\delta_3)$ only depends on τ_3 and δ_1, we have the following result.

Corollary 6: For $\tau_1 \leq \tau_2 \leq \tau_3$, $\delta_1 \leq \delta_2 \leq \delta_3$, $0 \leq \tau_i \leq \delta_i \leq 1$, we have

$$\mu(\tau_1,\tau_2,\tau_3,\delta_1,\delta_2,\delta_3) = \mu(\tau_3,\tau_3,\tau_3,\max\{\tau_3,\delta_1\},1,1).$$

□

We can thus conclude that asymptotically any error control combination can be upgraded to simultaneous symmetric error correction/detection and all unidirectional error detection, without losing rate. In other words, speaking of costs in terms of rate, we can say that correction of unidirectional and/or asymmetric errors is as expensive as correction of symmetric errors, while detection of unidirectional and/or asymmetric errors is free.

ACKNOWLEDGMENT

The author wishes to thank M. Blaum, C. de Vroedt, and the reviewers for valuable comments.

REFERENCES

[1] J. H. van Lint, *Introduction to Coding Theory*. New York: Springer-Verlag, 1982.

[2] J. H. Weber, C. de Vroedt, and D. E. Boekee, "Necessary and sufficient conditions on block codes correcting/detecting errors of various types," *IEEE Trans. Comput.*, vol. 41, pp. 1189–1193, Sept. 1992.

A Bounded-Distance Decoding Algorithm for Lattices Obtained from a Generalized Code Formula

Mauro A. O. da Costa e Silva, *Member, IEEE* and
Reginaldo Palazzo, Jr., *Member, IEEE*

Abstract—**A multistage decoding algorithm is given for lattices obtained from a multilevel code formula. The algorithm is shown to have the same effective error-correcting radius as maximum-likelihood decoding, so that the performance loss is essentially determined by the increase in the effective error coefficient, for which an expression is given. The code formula generalizes some previous multilevel constructions to constructions of known single-level binary lattices with many levels, and then to decoders for them with the proposed algorithm. The trade-off between complexity reduction and performance loss is evaluated for several known lattices and two new ones, indicating that the approach is effective provided the binary codes involved in the code formula are not too short.**

Index Terms—**Bounded-distance decoding, generalized code formula, complexity reduction, performance loss, lattices, maximum-likelihood decoding, effective error-correcting radius.**

I. INTRODUCTION

The recently intensified use of multidimensional lattices in block or trellis codes for bandlimited channels has focused the attention of many researchers on the problem of complexity reduction in lattice decoding [1]–[4], [6]. For multilevel binary lattices expressible in terms of code formulas based on the chain $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}/\cdots$ of two-way lattice partitions, Forney [5] has proposed a suboptimum algorithm that offers an advantageous compromise between complexity reduction and performance loss when the number of levels in the code formula is greater than one. However, the decoding of binary lattices with single-level code formulas like H_{16}, X_{24}, and X_{32} cannot benefit directly from this algorithm. The present work extends in some sense the previous approach by generalizing its multistage algorithm to more general code formulas based on chains of two-way lattice partitions other than $\mathbb{Z}/2\mathbb{Z}/4\mathbb{Z}/\cdots$, therefore achieving a broader range of trade-offs between complexity reduction and performance loss.

The ideas of multistage decoding and multilevel codes has been applied in various ways to the problems of complexity reduction and code construction. Imai and Hirakawa [10] introduced constructions using binary codes in multiple levels and proposed multistage decoders for them, showing that these decoders could achieve the same effective error correcting radius as ML decoding. Sayegh [11] constructed many signal sets using multilevel constructions based on two-way set partitions. Also, Ginzburg [12] proposed constructions based on multilevel partition chains. Calderbank [13] and Pottie and Taylor [16] designed multilevel codes using multilevel codes on multipart labels de-

---

Manuscript received August 4, 1992; revised September 12, 1994. This work was supported in part by the Conselho Nacional de Desenvolvimento Científico e Tecnológico under CNPq Grant 301416/85-0 and by the Fundação de Amparo à Pesquisa do Estado de São Paulo (FAPESP), Brazil, under Grant 92/4845-7. This paper was presented in part at the 1993 IEEE International Symposium on Information Theory, San Antonio, TX, Jan. 17–22, 1993.

M. A. O. da Costa e Silva is with the Department of Electrical Engineering, EESC-USP, 13560-250 São Carlos, SP, Brazil.

R. Palazzo, Jr., is with the Department of Communications, State University of Campinas-UNICAMP, 13081-970 Campinas, SP, Brazil.

IEEE Log Number 9406316.