Multiple Error Correction with Analog Codes[1]

Werner Henkel

Institut für Netzwerk- und Signaltheorie

Technische Hochschule Darmstadt

Merckstr. 25, D-6100 Darmstadt

1 Introduction

In 1983 J.K. Wolf wrote a paper titled "Redundancy, the Discrete Fourier Transform, and Impulse Noise Cancellation" [1], where he published some ideas on using RS- or BCH-codes based on complex numbers, later introduced as *"Analog Codes"* or *"DFT-Codes"* [2]. The paper treated a simple example for correction of single errors in noise, where the single error, called 'burst', had a much higher amplitude than the noise samples.

In this contribution, results on correcting multiple errors (bursts) are given, which analyze the influence of additive equally distributed or Gaussian noise on the error (burst) correction process. But firstly the expected benefits of coding with complex numbers are explained using a new idea of defining a syndrome by applying the divided difference scheme of the Newton method of interpolation. After giving some simulation results on the effect of additive noise, the sensitivity of the 'error search' is studied, which means, that a relation between relative errors (noise) in the time-domain codeword and relative errors in the inverse transform of the error locator polynomial is derived. Furthermore, it is shown, that the solutions of the Toeplitz subsystems which are generated during the execution of the recursive Berlekamp-Massey-Algorithm yield bounds for the condition numbers of the corresponding submatrices. These bounds are determined using the fact that the BMA leads to a triangular 'square-root' factorization of the inverse Toeplitz submatrices similar to that achieved by the Cholesky method for symmetric matrices.

2 Benefits of coding with complex numbers

In [1] a proof is given, that (almost always) *Analog Codes* are capable of correcting a number of errors equal to $M-1$, where M equals the number of parity samples.

Here, another proof is given based on the Newton-method of interpolation, also called interpolation by divided differences. This proof leads to a new way of defining a syndrome that reveals the special feature that an error-free range of the codeword can be detected from the syndrome without any further operations.

---

[1]Reprinted with minor corrections from Proc. 6th International Conference on Applied Algebra, Algebraic Algorithms, and Error Correcting Codes (AAECC-6), Springer Lecture Notes in Computer Science 357, 1989, pp. 239-249, The author is currently with Telecommunications Research Center Vienna (ftw.), Donau-City-Str. 1, A-1220 Vienna, Austria, E-mail: werner.henkel@ieee.org

An analog RS-codeword can be defined as samples x_i of a polynomial $X(\xi)$ of the form

$$x_i = X(z^{-i}) = \frac{1}{N}\sum_{k=0}^{K-1} X_k \cdot (z^{-i})^k\,, \quad z = e^{j\frac{2\pi}{N}}\,, \quad i = 0, \ldots, N-1\,, \tag{1}$$

which has a degree of $K-1$.

The divided differences of the Newton-method are given by

$$\Delta^1 x_i = \frac{x_{i+1} - x_i}{z^{-(i+1)} - z^{-i}} \tag{2}$$

$$\Delta^k x_i = \frac{\Delta^{k-1} x_{i+1} - \Delta^{k-1} x_i}{z^{-(i+k)} - z^{-i}}\,. \tag{3}$$

Analogous to the derivative of polynomials they have the property that

$$\Delta^K x_i = 0\,, \tag{4}$$

if $K-1$ is the degree of the polynomial (see e.g. [3]). With random errors of continuous value, it is nearly impossible that an erroneous codeword would be given according to a polynomial of degree $K-1$. It follows that a zero K'th divided difference is equivalent to a region of $K+1$ correct samples (see figure 1). Applying $\binom{N}{K+1}$ permutations at most, one can be sure that a zero appears at a special location in the syndrome of K'th divided differences if any $K+1 = N-M+1$ samples are error-free. This proves the error correction capability of analog codes and presents an interesting way of defining a syndrome. In the case of maximum number of errors $e_{max} = M-1$ a portion of $Ne_{max}!(N-e_{max})!/N! = N/\binom{N}{e_{max}}$ of all permutations yield the desired zero K'th divided difference.

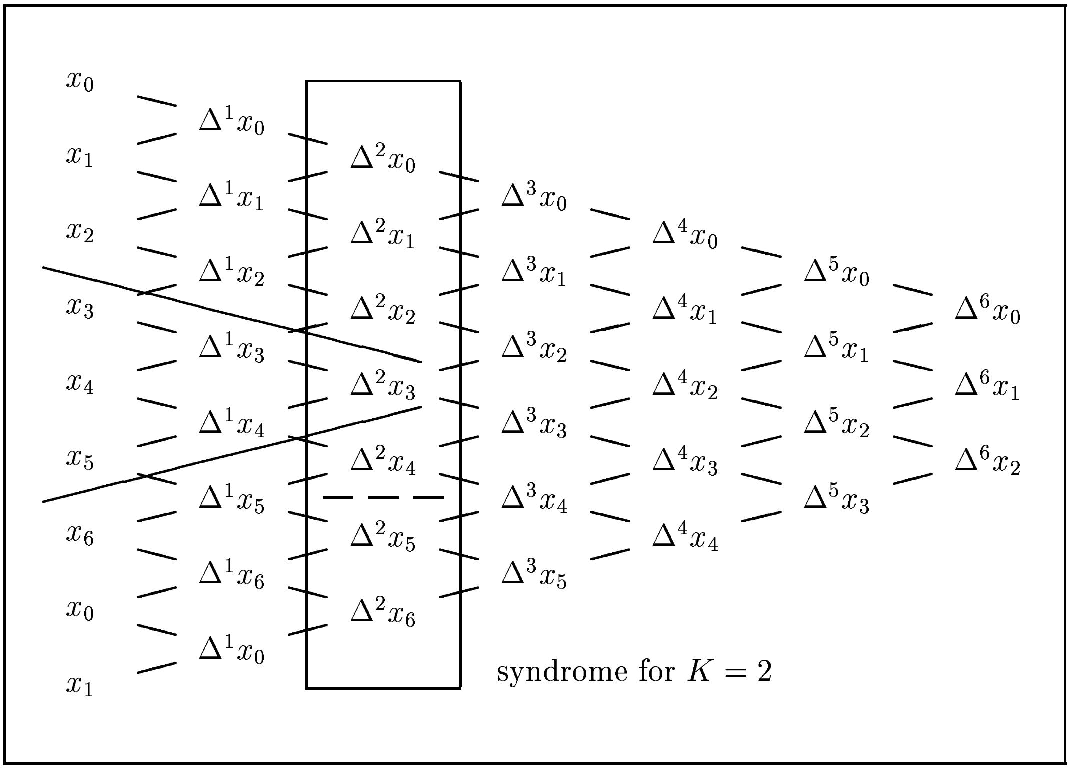

Figure 1: Scheme for the generation of divided differences

right direction. Besides the fact that more errors (bursts) may be correctable, *"Analog Codes"* have the property to be tolerant of background noise, if its amplitude is considerably lower than that of the 'bursts' to be corrected. There is no analogue for codes over Galois fields, because of the lack of magnitude relations in such finite fields.

This paper is especially devoted to the examination of the influence of additional noise in determining the error locations (solution of the key equation) by usual, algebraic methods. A treatment of the calculation of the error magnitudes has been omitted, because it is only an application of well-known interpolation or approximation methods, e.g. Lagrange-Interpolation, Newton-Method, Forney-Algorithm, recursion using the key equation, or least-squares approximation.

To start, computer simulations are studied to give a first impression.

3 Some simulation results

Simulation results are given, showing the influence of noise on the solution of the key-equation or the corresponding Toeplitz system. Firstly, we quote some results for the case of additive background noise with equally distributed amplitude (in an interval) and phase. Gaussian noise will be treated afterwards. The 'bursts' are restricted to be of constant amplitude and random, equally distributed phase.

Ideally, the 'bursts' are to be located by zeros in the coefficients of the inverse transform $c(\xi)$ of the error locator polynomial $C(\xi)$. With additional noise, no exact zeros would appear in that time-domain error locator. The minima of the samples will then represent the 'burst'-locations, which is far more practical than determining the exact complex zeros. So the quotient

$$Q = \frac{Min\{|c_i|_{\text{error-free locations}}\}}{Max\{|c_i|_{\text{error locations}}\}} \tag{5}$$

represents a measure for the quality of error detection. Figure 2 shows the dependence of this measure on the maximal amplitude of the noise (divided by the 'burst' amplitude) and the number of errors e. A hyperbolic relation becomes obvious. Note that for $Q > 1$ all e errors can be found and no error-free samples are taken for being erroneous.

Results for additive normally distributed noise are presented in figure 3. The portion of correctable error pattern (by solving the key equation) is shown as function of the standard deviation. Upper bounds are added, representing the probability of being able to distinguish 'bursts' from the noise. This probability is given by

$$P_d = P(\min\{\mathbf{z}_i | i \in U\} > \max\{\mathbf{z}_i | i \in \overline{U}\}), \tag{6}$$

where U symbolizes the set of indices of the 'burst'-locations, $\overline{U}$ the one without 'bursts', and $\mathbf{z}_i$ the random variables at location i. For illustration see figure 4. Omitting some steps of the derivation, the probability follows as

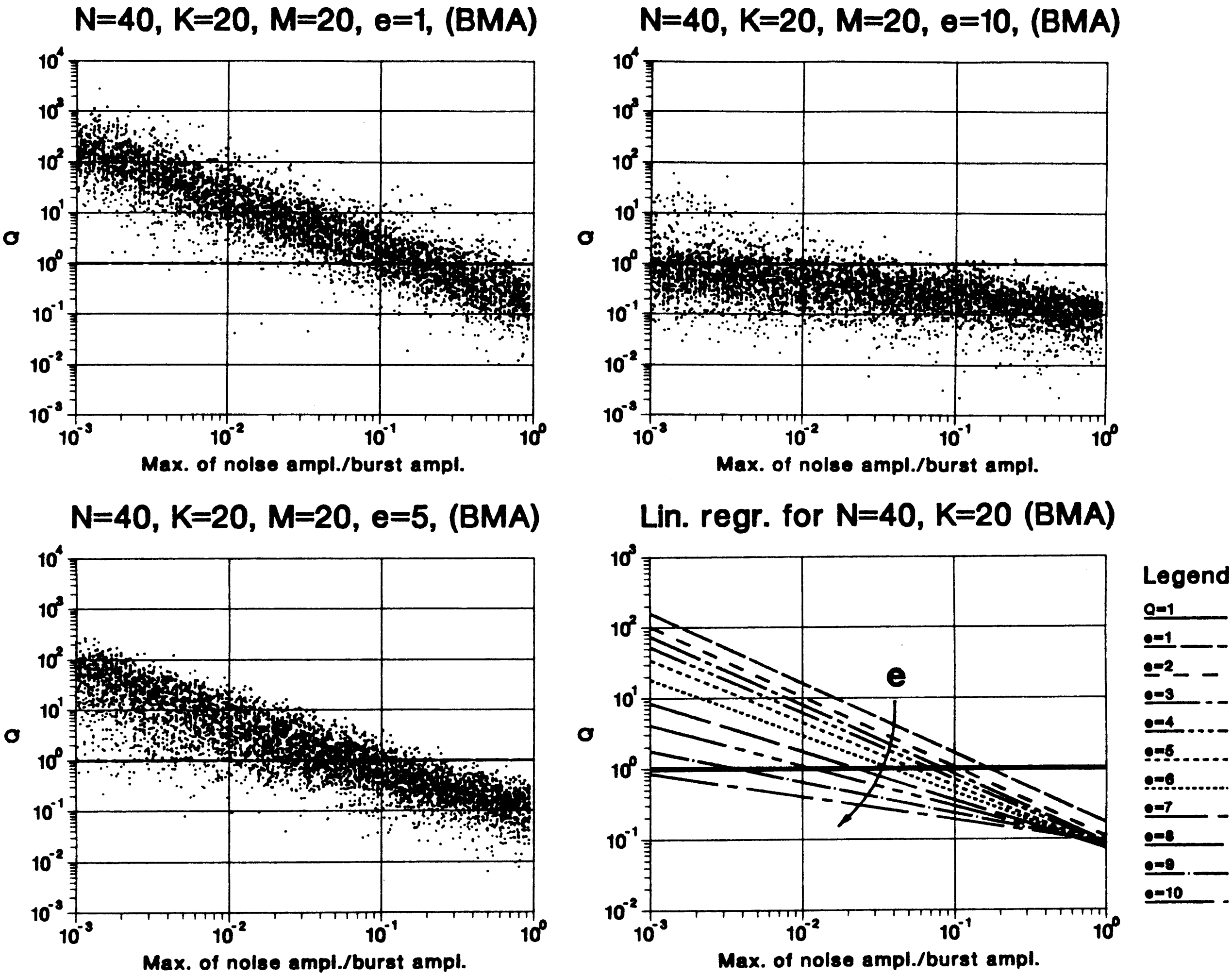

Figure 2: The influence of equally distributed noise on determining the error locations

$$P_d = \int_{u=-\infty}^{\infty} \left(F_{\mathbf{z}_{\overline{U}}}(u)\right)^{N-e} \cdot e \cdot \left(1 - F_{\mathbf{z}_U}(u)\right)^{e-1} \cdot f_{\mathbf{z}_U}(u)\, du \tag{7}$$

$$F_{\mathbf{z}_U}(u) = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{u-1}{\sqrt{2}\sigma}\right)\right) \tag{8}$$

$$F_{\mathbf{z}_{\overline{U}}}(u) = \frac{1}{2}\left(1 + \operatorname{erf}\left(\frac{u}{\sqrt{2}\sigma}\right)\right) \tag{9}$$

$$f_{\mathbf{z}_U}(u) = \frac{1}{\sqrt{2\pi}\sigma} e^{-(u-1)^2/(2\sigma^2)} \tag{10}$$

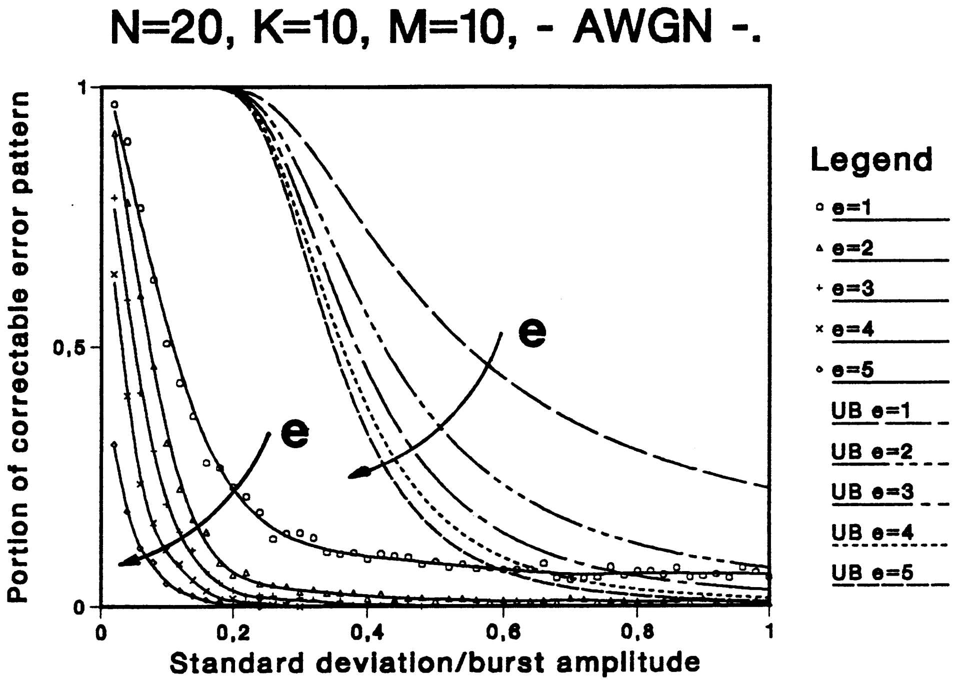

Figure 3: Portion of correctable error pattern under Gaussian noise

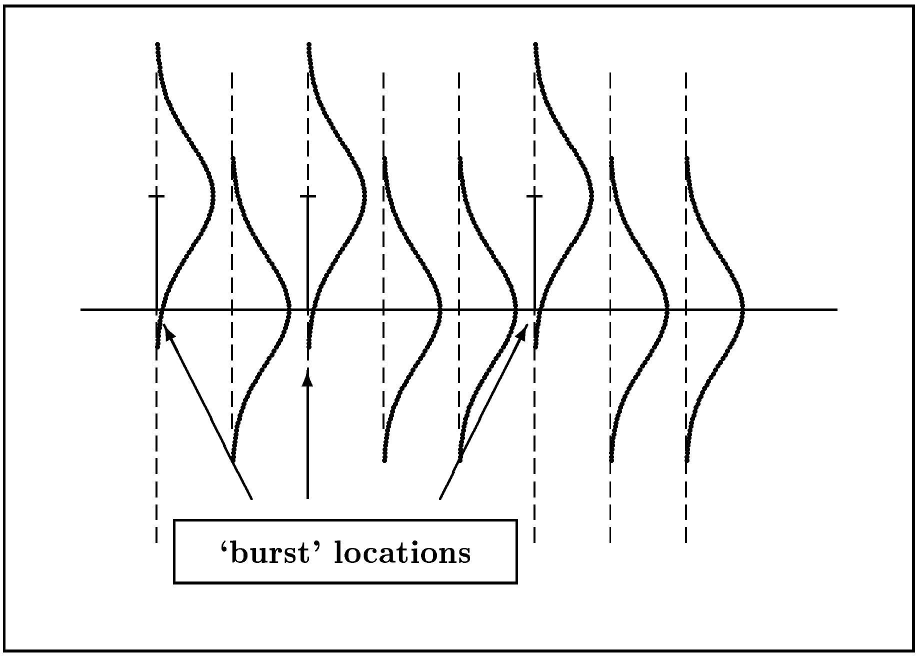

Figure 4: Illustration for derivation of upper bounds in (6)

4 The sensitivity of the 'error search'

The 'error search' consists of three main operations:

I Transform of the time-domain codeword ($\vec{f}$) into the frequency domain ($\vec{F}$)
– *DFT* –

$$\vec{F} = \underline{Z}_{N\times N}\vec{f} \qquad \underline{Z}_{N\times N} = \begin{pmatrix} 1 & 1 & 1 & \cdots \\ 1 & z^1 & z^2 & \\ 1 & z^2 & z^4 & \\ \vdots & & & \end{pmatrix} \tag{11}$$

II Extraction of the syndrome $(S_0, S_1, \ldots, S_{2e-1})$ from $\vec{F}$ and solution of the Hankel (Toeplitz) system

$$\begin{pmatrix} S_{2e-2} & S_{2e-3} & \cdots & S_{e-1} \\ S_{2e-3} & & & \vdots \\ \vdots & & & \vdots \\ S_{e-1} & \cdots & \cdots & S_0 \end{pmatrix} \begin{pmatrix} C_1 \\ C_2 \\ \vdots \\ C_e \end{pmatrix} = - \begin{pmatrix} S_{2e-1} \\ S_{2e-2} \\ \vdots \\ S_e \end{pmatrix} . \tag{12}$$

In abbreviated form

$$\underline{S} \cdot \vec{C} = -\vec{s}$$

III Inverse transform of the error locator

– DFT^{-1} –

$$\vec{c} = \underline{Z}_{N\times e}^{-1}\vec{C} \qquad \underline{Z}_{N\times e}^{-1} = \frac{1}{N}\left.\overbrace{\begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & z^{-1} & z^{-2} & & \\ 1 & z^{-2} & z^{-4} & & \\ \vdots & & & & \\ \vdots & & & & \end{pmatrix}}^{e+1}\right\} N \tag{13}$$

These three steps will now be studied to achieve an approximate relationship for the relative error $\rho_{\vec{c}}$ of the error locator $\vec{c}$ as function of the relative error $\rho_{\vec{f}}$ of the time-domain codeword $\vec{f}$ ($\rho_{\vec{c}} = \| \Delta\vec{c} \|_\infty / \| \vec{c} \|_\infty$, $\rho_{\vec{f}} = \| \Delta\vec{f} \|_\infty / \| \vec{f} \|_\infty$).

For the DFT-Matrices we obtain

$$\| \underline{Z}_{N\times N} \|_\infty = N\,, \quad \| \underline{Z}_{N\times N}^{-1} \|_\infty = \frac{N}{N} = 1\,,$$

$$\| \underline{Z}_{N\times e}^{-1} \|_\infty = \frac{e}{N}\,, \quad \| \underline{Z}_{e\times N} \|_\infty = N\,. \tag{14}$$

First step

If $\epsilon\vec{e}$ represents the noise vector and the index i stands for the 'bursty' vectors without background noise, it follows that

$$\vec{F} = \underline{Z}_{N\times N}\vec{f} = \underline{Z}_{N\times N}(\vec{f}_i + \epsilon\vec{e}) \tag{15}$$

$$\Longrightarrow \Delta\vec{F} = \underline{Z}_{N\times N} \cdot \epsilon\vec{e} \tag{16}$$

$$\Longrightarrow \| \Delta\vec{F} \| \leq \| \underline{Z}_{N\times N} \| \cdot \epsilon \cdot \| \vec{e} \|\,, \tag{17}$$

Furthermore,

$$\vec{f}_i = \underline{Z}_{N\times N}^{-1}\vec{F}_i \tag{18}$$

$$\Longrightarrow \| \vec{f}_i \| \leq \| \underline{Z}_{N\times N}^{-1} \| \cdot \| \vec{F}_i \| \quad \Longrightarrow \quad \frac{\| \underline{Z}_{N\times N}^{-1} \| \cdot \| \vec{F}_i \|}{\| \vec{f}_i \|} \geq 1 \tag{19}$$

Combining relations (17) and (19) we get

$$\| \Delta\vec{F}_i \| \leq \| \underline{Z}_{N\times N} \| \cdot \epsilon \cdot \| \vec{e} \| \, \frac{\| \underline{Z}_{N\times N}^{-1} \| \cdot \| \vec{F}_i \|}{\| \vec{f}_i \|} \tag{20}$$

$$\Longrightarrow \frac{\| \Delta\vec{F} \|}{\| \vec{F}_i \|} \leq \underbrace{\| \underline{Z}_{N\times N} \| \cdot \| \underline{Z}_{N\times N}^{-1} \|}_{\kappa\{\underline{Z}_{N\times N}\}} \cdot \frac{\epsilon \, \| \vec{e} \|}{\| \vec{f}_i \|}\,, \tag{21}$$

$$\rho_{\vec{F}} \le \kappa\{\underline{Z}_{N\times N}\} \cdot \rho_{\vec{f}}, \tag{22}$$

where $\kappa\{\underline{Z}_{N\times N}\}$ is the condition number of $\underline{Z}_{N\times N}$.

Second step

Regarding the Hankel (Toeplitz) system

$$\underline{S} \cdot \vec{C} = -\vec{s}, \tag{23}$$

we obtain according to [4]

$$\frac{\| \Delta\vec{C} \|}{\| \vec{C}_i \|} \le \underbrace{\| \underline{S} \| \cdot \| \underline{S}^{-1} \|}_{\kappa\{\underline{S}\}} \cdot (\rho_A + \rho_B) \ \left(+O(\epsilon^2)\right), \tag{24}$$

with

$$\rho_A = \frac{\| \Delta\underline{S} \|}{\| \underline{S}_i \|} \quad \text{and} \quad \rho_B = \frac{\| \Delta\vec{s} \|}{\| \vec{s}_i \|}$$

Using the L_∞-Norm and taking into account that $\vec{s}$ is just a section of $\vec{F}$ we obtain

$$\rho_B = \frac{\| \Delta\vec{s} \|_\infty}{\| \vec{s}_i \|_\infty} = \frac{\| \Delta\vec{s} \|_\infty}{\| \vec{F}_i \|_\infty} \cdot \frac{\| \vec{F}_i \|_\infty}{\| \vec{s}_i \|_\infty} \le \rho_{\vec{F}} \cdot \frac{\| \vec{F}_i \|_\infty}{\| \vec{s}_i \|_\infty}. \tag{25}$$

Similar considerations for ρ_A yield

$$\rho_A = \frac{\| \Delta\underline{S} \|_\infty}{\| \underline{S}_i \|_\infty} \le e \cdot \rho_{\vec{F}} \cdot \frac{\| \vec{F}_i \|_\infty}{\| \underline{S}_i \|_\infty}. \tag{26}$$

Third step

Analogous to the first step, the inverse Transform of the error locator

$$\vec{c} = \underline{Z}^{-1}_{N\times e}\vec{C} \tag{27}$$

leads to

$$\frac{\| \Delta\vec{c} \|}{\| \vec{c}_i \|} \le \| \underline{Z}^{-1}_{N\times e} \| \cdot \| \underline{Z}_{e\times N} \| \cdot \frac{\| \Delta\vec{C} \|}{\| \vec{C}_i \|}. \tag{28}$$

Combining the results already obtained, the relative error $\rho_{\vec{c}} = \frac{\|\Delta\vec{c}\|_\infty}{\|\vec{c}_i\|_\infty}$ of the error locator in the 'time-domain' is given by (all norms are L_∞ norms)

$$\frac{\| \Delta\vec{c} \|}{\| \vec{c}_i \|} \le \| \underline{Z}^{-1}_{N\times e} \| \cdot \| \underline{Z}_{e\times N} \| \cdot \| \underline{S} \| \cdot \| \underline{S}^{-1} \| \cdot \left(\frac{\| \vec{F}_i \|}{\| \vec{s}_i \|} + e \frac{\| \vec{F}_i \|}{\| \underline{S}_i \|} \right) \cdot \tag{29}$$

$$\cdot \| \underline{Z}_{N\times N} \| \cdot \| \underline{Z}^{-1}_{N\times N} \| \cdot \frac{\epsilon \| \vec{e} \|}{\| \vec{f}_i \|} =$$

$$\Longrightarrow \rho_{\vec{c}} \leq e \cdot N \cdot \kappa\{\underline{S}\} \cdot \left(\frac{\| \vec{F}_i \|_\infty}{\| \vec{s}_i \|_\infty} + e \frac{\| \vec{F}_i \|_\infty}{\| \underline{S}_i \|_\infty} \right) \cdot \rho_{\vec{f}} \tag{30}$$

Knowing that bounds obtained from condition considerations are gross overestimations in general, (30) could be approximated by

$$\boxed{\rho_{\vec{c}} \leq 2(e+1)N \cdot \kappa\{\underline{S}\} \cdot \rho_{\vec{f}}} \tag{31}$$

(Simulations showed this approximated bound to be a gross one, too.)

5 Bounds for the condition numbers of Hankel (Toeplitz) submatrices used during execution of Berlekamp's algorithm (BMA)

The last section showed that the bound for the relative error $\rho_{\vec{c}}$ of the time-domain error locator is especially dependent on the condition number $\kappa\{\underline{S}\}$ of the syndrome matrix. Now bounds for $\kappa\{\underline{S}\}$ are derived using parameters that are directly available during execution of Berlekamp's recursive algorithm ([5]). For this, the fact is used that BMA leads to a triangular 'square root'-factorization.

For *"Analog Codes"* the usual BMA has to be modified slightly. The check on discrepancy equal or not equal to zero has to be replaced by a threshold decision like '**IF** $\mathbf{d} < \mathbf{d_0}$ **THEN**' with an appropriately chosen d_0. Another possibility is to skip that operation totally, which means setting d unequal to zero always. In that case, every second recursion, the BMA yields a system of linear equations (before each length change) of the form

$$(1, C_1, C_2, \ldots, C_l) \begin{pmatrix} S_l & & S_{2l} \\ & \ddots & \\ S_0 & & S_l \end{pmatrix} = (0, \ldots, 0, d_{2l}) \tag{32}$$

$$\Longleftrightarrow \underbrace{\begin{pmatrix} S_{2l} & & S_l \\ & & \\ S_l & & S_0 \end{pmatrix}}_{=: \underline{S}_l} \begin{pmatrix} 1 \\ C_1 \\ \vdots \\ C_l \end{pmatrix} = \begin{pmatrix} d_{2l} \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \tag{33}$$

where d_{2l} is a discrepancy before a length change and the vector $(1, C_1, \ldots, C_l)$ consists of the corresponding coefficients of the error locator polynomial, we obtain

$$(S_e)\cdot\underbrace{\begin{pmatrix} 1 & 0 & 0 & 0 \\ C_{e,1} & 1 & 0 & 0 \\ \vdots & & \ddots & 0 \\ C_{e,e} & C_{e-1,e-1} & \cdots & 1 \end{pmatrix}}_{=:\underline{C}_e} = \begin{pmatrix} d_{2e} & \cdot & \cdot & \cdot \\ 0 & \ddots & \cdot & \cdot \\ 0 & 0 & d_2 & \cdot \\ 0 & 0 & 0 & d_0 \end{pmatrix}. \tag{34}$$

$$\Longrightarrow \underline{C}_e^T\cdot\underline{S}_e\cdot\underline{C}_e = \begin{pmatrix} d_{2e} & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_2 & 0 \\ 0 & 0 & 0 & d_0 \end{pmatrix} \tag{35}$$

The promised factorization follows:

$$\boxed{\underline{S}_e^{-1} = \underline{C}_e\underline{D}_e^{-1}\underline{C}_e^T \quad \text{or} \quad \underline{S}_e = (\underline{C}_e^T)^{-1}\underline{D}_e\underline{C}_e^{-1}} \tag{36}$$

$$\underline{C}_e = \begin{pmatrix} 1 & 0 & 0 & 0 \\ C_{e,1} & 1 & 0 & 0 \\ \vdots & & \ddots & 0 \\ C_{e,e} & C_{e-1,e-1} & \cdots & 1 \end{pmatrix} \quad \underline{C}_e^T = \begin{pmatrix} 1 & C_{e,1} & \cdots & C_{e,e} \\ 0 & 1 & & \vdots \\ 0 & 0 & \ddots & \vdots \\ 0 & 0 & 0 & 1 \end{pmatrix} \tag{37}$$

$$\underline{D}_e = \begin{pmatrix} d_{2e} & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & d_2 & 0 \\ 0 & 0 & 0 & d_0 \end{pmatrix} \quad \underline{D}_e^{-1} = \begin{pmatrix} 1/d_{2e} & 0 & 0 & 0 \\ 0 & \ddots & 0 & 0 \\ 0 & 0 & 1/d_2 & 0 \\ 0 & 0 & 0 & 1/d_0 \end{pmatrix}, \tag{38}$$

where the d_{2l} are the discrepancies before the last length change and the columns of $\underline{C}_e$ are the corresponding coefficients of the error locator polynomial.

An interesting point is that the Cholesky-method achieves a similar triangular 'square-root' factorization.

By using relation (36), bounds for $\| \underline{S}_e^{-1} \|_\infty$, $\| \underline{S}_e \|_\infty$ and $\kappa\{\underline{S}_e\}$ are given by:

$$\| \underline{S}_e^{-1} \|_\infty \geq \frac{1}{|d_{2e}|}(1 + |C_{e,1}| + \cdots + |C_{e,e}|) \tag{39}$$

$$\| \underline{S}_e \|_\infty \geq |d_0| \tag{40}$$

$$\kappa\{\underline{S}_e\} \geq \frac{|d_0|}{|d_{2e}|}(1 + |C_{e,1}| + \cdots + |C_{e,e}|) \tag{41}$$

and likewise

$$\kappa\{\underline{S}_e\} \leq \kappa\{\underline{C}_e\}\kappa\{\underline{C}_e^T\}\frac{\max |d_{2i}|}{\min |d_{2i}|} \tag{42}$$

For this derivation of bounds only parameters are used, that are directly available from BMA

6 Conclusions

After pointing out the expected advantages of complex coding compared to usual RS- or BCH-codes over finite fields, it has been shown that *"Analog Codes"* are able to correct multiple errors (bursts) also if additional background noise is superimposed. Simulations made obvious that the amplitude of the noise has to be of considerably lower amplitude than the 'bursts' to be corrected. Furthermore, it has been stated that intermediate solutions during execution of the recursive Berlekamp-Massey-Algorithm are not meaningless but represent a measure for the conditioning of the corresponding sub-Toeplitz system.

References

[1] Wolf, J.K., "Redundancy, the Discrete Fourier Transform, and Impulse Noise Cancellation", *IEEE Trans. on Comm.*, vol. COM-31, No. 3, pp. 458-461, March 1983.

[2] Wolf, J.K., "Analog Codes", *IEEE Int. Conf. on Comm. (ICC '83)*, Boston, MA, USA, 19-22 June 1983, pp. 310-12 vol. 1.

[3] Hildebrandt, F.B., *Introduction to numerical analysis*, McGraw-Hill, New York, Toronto, London, 1956.

[4] Golub, G.H., van Loan, C.F., *Matrix Computations*, North Oxford Academic Publishing, Oxford, 1983

[5] Massey, J.L., "Shift-Register Synthesis and BCH Decoding", *IEEE Trans. on Inf. Theory*, vol. IT-15, No. 1, pp. 122-127, January 1969.

[6] Marshall, T.G., "Real number transform and convolutional codes", in *Proc. 24th Midwest Symp. Circuits Syst.*, S. Karne, Ed., Albuquerque, NM, June 29-30, 1981.

[7] Maekawa, Y., Sakaniwa, K., "An Extension of DFT Code and the Evaluation of its Performance", *Int. Symp. on Information Theory*, Brighton, England June 24-28, 1985.

[8] Cybenko, G., "The numerical stability of the Levinson-Durbin Algorithm for Toeplitz systems of equations", *SIAM J. Sci. Stat. Comput.*, vol. 1, No. 3, pp. 303-319, September 1980.