ACKNOWLEDGMENT

The authors wish to thank Prof. E. F. Assmus for his careful and patient reading which improved the quality of the paper.

REFERENCES

[1] D. Augot, P. Charpin, and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inform. Theory*, vol. 38, pp. 960–973, May 1992.
[2] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error Correcting Codes.* Amsterdam: North-Holland, 1977.
[3] W. W. Peterson and E. J. Weldon, Jr., *Error-Correcting Codes.* Cambridge, MA: M.I.T. Press, 1972.
[4] J. H. van Lint and R. M. Wilson, "On the minimum distance of cyclic codes," *IEEE Trans. Inform. Theory,* vol. IT-32, pp. 23–40, Jan. 1986.

Codes Over Gaussian Integers

Klaus Huber

***Abstract*—In this contribution it is shown how block codes over Gaussian integers can be used for coding over two-dimensional signal space. We introduce a two-dimensional modular distance called Mannheim distance and propose using codes designed for this distance. Some simple constructions of such codes are given, among them icyclic codes which belong to the class of constacyclic codes. As a special case icyclic codes include perfect one Mannheim error correcting codes. For most of the codes considered efficient decoders are given and their performance on the Gaussian channel is investigated.**

***Index Terms*— Block codes, Gaussian integers, sum of two squares, Manhattan distance, Mannheim distance, QAM signal constellations.**

I. INTRODUCTION

It is well known that the beautiful algebraic theory of block codes over finite fields does have severe problems with coding for two-dimensional signal constellations such as quadrature amplitude modulation (QAM). This is mainly due to the fact that in two (or higher) dimensions the usual Hamming distance is inappropriate. For phase shift keyed (PSK) signals block codes using the Lee distance provide a good solution, whereas neither Hamming nor Lee distance are adequate for handling QAM signals.

To improve the situation in the two-dimensional case we introduce the Mannheim distance which is the Manhattan distance modulo a two-dimensional grid.

Then we propose block codes over Gaussian integers designed for the Mannheim distance which are suited for QAM signals. The main class of codes considered are icyclic codes which belong to the class of constacyclic codes ([1, p. 303]). We show the power of these codes when used with the Mannheim metric. First decoders are developed which are able to correct Mannheim errors of weight one and two. These decoders work in a similar way as the decoders for negacyclic codes for the Lee distance given by Berlekamp in ([1, pp. 207–217]). Then codes are considered which can correct more than two Mannheim errors. The gain of the codes on a Gaussian channel is also investigated.

II. CODES OVER GAUSSIAN INTEGERS

Gaussian integers are a subset of complex numbers which have integers as real and imaginary parts. Fermat's well-known and famous two square theorem tells us that primes of the form $p \equiv 1 \bmod 4$ can be written in essentially one way as a sum of two squares (see, e.g., [3, Theorem 251]). Hence such primes p are the product of two conjugate complex Gaussian integers:

$$p = a^2 + b^2 = \pi \cdot \pi^* \tag{1}$$

where $\pi = a + i \cdot b$ and the conjugate of π is $\pi^* = a - i \cdot b$. The properties of Gaussian integers as relevant for this paper are listed in Appendix E, for further details see, e.g., [3, pp. 182–187], a fast algorithm to compute a and b for a given p can be found in Appendix F. Let $\mathcal{G}$ be the Gaussian Integers and $\mathcal{G}_\pi$ the residue class of $\mathcal{G}$ modulo π, where the modulo function $\mu\colon \mathcal{G} \rightarrow \mathcal{G}_\pi$ is defined according to

$$\mu(\xi) = \xi \bmod \pi = \eta = \xi - \left[\frac{\xi \cdot \pi^*}{\pi \cdot \pi^*}\right] \cdot \pi. \tag{2}$$

$[\cdot]$ denotes rounding of complex numbers which is defined in Appendix E such that the norm of η is as small as possible (i.e., the energy of the corresponding signal point is as small as possible). In Figs. 1–6 the sets $\mathcal{G}_\pi$ obtained from the primes $p = 5$, 13, 17, 29, 37, and 41 are displayed as points in the complex plane. Having coding for communication channels in mind we call these two-dimensional visualisations of $\mathcal{G}_\pi$ by the communication term *signal constellation.* Similarly, as for ordinary integers, we can employ the extended Euclidean algorithm for Gaussian integers to compute u and v which fulfill

$$1 = u \cdot \pi + v \cdot \pi^*. \tag{3}$$

Table VIII gives π, u, and v for the primes $p \equiv 1 \bmod 4$ and $p \leq 113$. The modulo function μ defines a bijective mapping from $GF(p)$ into two-dimensional signal space $\mu\colon GF(p) \rightarrow \mathcal{G}_\pi$

$$\mu(g) = g \bmod \pi = \gamma = g - \left[\frac{g \cdot \pi^*}{p}\right] \cdot \pi. \tag{4}$$

Using (3) we immediately get the inverse mapping μ^{-1} as

$$g = \mu^{-1}(\gamma) \equiv \gamma \cdot (v\pi^*) + \gamma^* \cdot (u\pi) \bmod p, \tag{5}$$

for if g is an integer of $GF(p)$ then $g = \kappa \cdot \pi + \gamma$ and $g = g^* = \kappa^* \cdot \pi^* + \gamma^*$, hence, $\gamma \cdot (v\pi^*) + \gamma^* \cdot (u\pi) = (g - \kappa\pi) \cdot (v\pi^*) + (g - \kappa^*\pi^*) \cdot (u\pi) \equiv g \cdot (v\pi^* + u\pi) \bmod p$ which equals g by (3).

Clearly, μ defines an isomorphism, namely, $\mu(g_1 + g_2) = \mu(g_1) + \mu(g_2)$ and $\mu(g_1 \cdot g_2) = \mu(g_1) \cdot \mu(g_2)$. Although $GF(p)$ and $\mathcal{G}_\pi$ are equivalent mathematically, we will see in the following sections that the field $GF(p)$ when represented as $\mathcal{G}_\pi$ offers significant technical advantages for coding over two-dimensional signal space. We therefore use $\mathcal{G}_\pi$ to stress this fact.

We now define a block code $\mathcal{C}$ of length n over the Gaussian integers $\mathcal{G}_\pi$ as a set of codewords $\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1})$ with coefficients $c_i \in \mathcal{G}_\pi$. In the following, we will mainly consider linear codes.

Manuscript received May 21, 1992. This work was presented in part at CDS-92 Conference, Kaliningrad (Königsberg), Russia, September 7–11, 1992, and at the IEEE Symposium on Information Theory, San Antonio, TX, January 17–22, 1993.

The author is with Deutsche Bundespost Telekom, Research Institute FZ123a, 64276 Darmstadt, Germany.

IEEE Log Number 9215213.

III. One Mannheim Error Correcting Codes

We first introduce the Mannheim distance. Let $\alpha, \beta \in \mathcal{G}_\pi$ and $\gamma = \beta - \alpha \bmod \pi$, and let the Mannheim weight of γ be defined as

$$w_M(\gamma) = |\mathrm{Re}\,(\gamma)| + |\mathrm{Im}\,(\gamma)|,$$

then the Mannheim distance d_M between α and β is defined as

$$d_M(\alpha, \beta) = w_M(\gamma). \tag{6}$$

Note that for $\alpha \in \mathcal{G}_\pi$ the Mannheim distance $d_M(\alpha, 0)$ equals the so-called Manhattan distance. Fig. 8 shows the difference between Manhattan and Mannheim distance modulo $\pi = 4 + i$. Fig. 9 motivates the naming chosen. As can be seen in Fig. 9 Mannheim like Manhattan has a very regular rectangular street map. It is also much smaller than Manhattan which symbolizes the modulo operation, and finally the beginning of the names Mannheim and Manhattan coincide. The Mannheim weight of the vector $\boldsymbol{x} = (x_0, x_1, \cdots, x_{n-1})$ over $\mathcal{G}_\pi$ is given by

$$w_M(\boldsymbol{x}) = \sum_{j=0}^{n-1} w_M(x_j),$$

and the Mannheim distance of $\boldsymbol{x}$ and $\boldsymbol{y}$ by $w_M(\boldsymbol{y} - \boldsymbol{x})$. The Mannheim distance like the Manhattan distance defines a metric, as $d(\boldsymbol{x}, \boldsymbol{y}) = d(\boldsymbol{y}, \boldsymbol{x})$, $d(\boldsymbol{x}, \boldsymbol{y}) \geq 0$ with equality if $\boldsymbol{x} = \boldsymbol{y}$, and $d(\boldsymbol{x}, \boldsymbol{z}) \leq d(\boldsymbol{x}, \boldsymbol{y}) + d(\boldsymbol{y}, \boldsymbol{z})$. The parameter $d_{\max}$ defined as

$$d_{\max} = \max\{d_M(\gamma, 0) | \gamma \in \mathcal{G}_\pi\}, \tag{7}$$

gives the maximum Mannheim distance which two elements of $\mathcal{G}_\pi$ can have. We get

$$d_{\max} = \max\{a, b\} - 1.$$

To see this, first note that for any $\chi \in \mathcal{G}_\pi$ we have $[\chi\pi^*/p] = 0$, which leads to $d_{\max} \leq \max\{a, b\} - 1$. Without loss of generality assume $a > b \geq 0$, then setting $\chi = (a-b-1)/2 + i(a+b-1)/2 \in \mathcal{G}_\pi$ we get equality (recall that as p is odd either a is even and b odd or a is odd and b even). In Table VIII $d_{\max}$ is given for all primes $p \equiv 1 \bmod 4$ and $p \leq 113$.

We start with the design of one Mannheim error correction (OMEC) codes of length $n = (p-1)/4$ which are able to correct errors of Mannheim weight one. A Mannheim error of weight one takes on one of the four values ±1, $\pm i$ at position $l (0 \leq l \leq n-1)$. Let $\alpha \in \mathcal{G}_\pi$ be an element of order $p - 1$. Now OMEC codes can be constructed by the following parity-check matrix $\boldsymbol{H}$:

$$\boldsymbol{H} = (\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{(p-1)/4)-1}). \tag{8}$$

Codewords are all vectors $\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1})$ over $\mathcal{G}_\pi$ which give $\boldsymbol{H} \cdot \boldsymbol{c}^\top = \boldsymbol{0}$. The corresponding generator matrix $\boldsymbol{G}$ is given by

$$\boldsymbol{G} = \begin{pmatrix} -\alpha^1, & 1, & 0, & \cdots, & 0 \\ -\alpha^2, & 0, & 1, & \cdots, & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ -\alpha^{(p-1)/4)-1}, & 0, & 0, & \cdots, & 1 \end{pmatrix}. \tag{9}$$

That the code $\mathcal{C}$ defined by the above matrix $\boldsymbol{H}$ is able to correct any Mannheim error of weight one is immediate as $\{\alpha^n, \alpha^{2n}, \alpha^{3n}, \alpha^{4n}\} = \{\pm 1, \pm i\}$. Hence, any single error from $\{1, -1, i, -i\}$ will produce a different syndrome. Decoding is straightforward. Take the received vector $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ and compute the syndrome $(s) = \boldsymbol{H} \cdot \boldsymbol{r}^\top$, the location of an error having $w_M(\boldsymbol{e}) = 1$ is then given by $l = \log_\alpha s \bmod n$ and its value by $s \cdot \alpha^{-l}$. Note that the OMEC codes are very efficient, as only one check symbol is needed to correct a Mannheim error of weight one. In Tables I–VII exponent tables of some small fields, and in Table VIII a primitive element α and $d_{\max}$ for the primes $p \equiv 1 \bmod 4$ with $p \leq 113$ are given.

We now consider a simple example.

Example 1: Let $p = 13$, $\pi = 3 + i \cdot 2$ and $\alpha = 1 + i$, then

$$\boldsymbol{H} = (1, 1+i, 2i)$$
$$\boldsymbol{G} = \begin{pmatrix} -(1+i), & 1, & 0 \\ -2 \cdot i, & 0, & 1 \end{pmatrix}.$$

Let us assume that at the receiving end we get the vector $\boldsymbol{r} = (1 + i, i, -1 + i)$, then $s = \boldsymbol{H} \cdot \boldsymbol{r}^\top = -2 = \alpha^{11}$, and we find that at position $2 = 11 \bmod 3$ we have an error value of $s \cdot \alpha^{-2} = i \Rightarrow \boldsymbol{e} = (0, 0, i), \Rightarrow \boldsymbol{c} = \boldsymbol{r} - \boldsymbol{e} = (1 + i, i, -1)$.

The codes defined by the parity check matrix of (8) can be generalized to the lengths $n = (p^r - 1)/4$ called primitive lengths in analogy to BCH and Berlekamp's negacyclic codes. The parity check matrix is then given by

$$\boldsymbol{H} = (\alpha^0, \alpha^1, \alpha^2, \cdots, \alpha^{(p^r-1)/4)-1}) \tag{10}$$

where $\alpha \in \mathcal{G}_{\pi^r}$ is an element of order $p^r - 1$. $\mathcal{G}_{\pi^r}$ denotes the field isomorphic to $GF(p^r)$. Similar to the usual Hamming distance codes we characterize linear Mannheim error correcting codes by the triple $[n, k, d_M]$ where n is the length, k the dimension, and

$$d_M = \min\{w_M(\boldsymbol{c}) | \boldsymbol{c} \neq \boldsymbol{0}, \boldsymbol{c} \in \mathcal{C}\} \tag{11}$$

the minimum Mannheim distance of the code.

To summarize, see the following.

Definition 1: $[n, n - r, 3]$ OMEC codes are block codes over $\mathcal{G}_\pi$ defined by the $\boldsymbol{H}$ matrix of (10) having length $n = (p^r - 1)/4$, dimension $k = n - r$ and minimum Mannheim distance $d_M = 3$ for primes $p \equiv 1 \bmod 4$.

To illustrate the construction in the extension field $\mathcal{G}_{\pi^r}$ we consider another example.

Example 2: Let $p = 5$, $\pi = 2 + i$, and $r = 2$. To construct $\mathcal{G}_{\pi^2}$ we use the primitive polynomial $p(x) = x^2 + x - i$. Then by (10) the parity check matrix

$$\boldsymbol{H} = \begin{pmatrix} 0, & 1, & -1, & 1+i, & 1-i, & -1 \\ 1, & 0, & i, & -i, & -1+i, & 1+i \end{pmatrix}, \tag{12}$$

leads to a [6, 4, 3] OMEC code. To decode the received vector $\boldsymbol{r} = (1, 0, 1 + i, 0, 0, 0)$ we compute

$$\boldsymbol{H} \cdot \boldsymbol{r}^\top = \begin{pmatrix} -1-i \\ i \end{pmatrix}.$$

Thus, $s = (-1 - i, i) = \alpha^{15}$ (see Table VII), i.e., at position $3 = 15 \bmod 6$ we have an error with value $\alpha^{12} = -1$ and the closest codeword is $\boldsymbol{c} = (1, 0, 1 + i, 1, 0, 0)$.

By sphere-packing we get

$$p^{n-r} \cdot (4n + 1) = p^{n-r} \cdot p^r = p^n.$$

Hence, the OMEC codes defined by (10) are *perfect*.

We finish this section by showing how the OMEC codes perform on the Gaussian channel. OMEC codes have $d_M = 3$, hence the smallest Euclidean distance d_E between two codewords is bounded by $d_E \geq \sqrt{3}$ which results in an asymptotic coding gain of

$$G = 10 \log_{10}\left(\frac{n-r}{n} \cdot 3\right) \text{ dB}$$
$$< G_{\max} = 10 \log_{10}(3) \text{ dB} \approx 4.77 \text{ dB}.$$

Asymptotic coding gain means for high signal-to-noise ratio (see, e.g., [2, p. 238] for further details). $G_{\max}$ gives the asymptotic coding gain for very long codes where the code rate $R = (n-r)/n$ tends to unity.

IV. Mannheim Error Correcting Codes having $d_M \geq 3$

We are interested in constructing codes which are able to correct errors of Mannheim weight greater than one. Therefore, we consider the code $\mathcal{C}$ defined by the following parity check matrix $\boldsymbol{H}$:

$$\boldsymbol{H} = \begin{pmatrix} \beta^0, & \beta^1, & \beta^2, & \cdots, & \beta^{n-1} \\ \beta^0, & \beta^5, & \beta^{10}, & \cdots, & \beta^{(n-1)5} \\ \vdots & & & & \vdots \\ \beta^0, & \beta^{(4t+1)}, & \beta^{2(4t+1)}, & \cdots, & \beta^{(n-1)(4t+1)} \end{pmatrix}. \qquad (13)$$

Let $\beta \in \boldsymbol{G}_{\pi^r}$ be an element of order $4n$ and $\beta^n = i$. Using $(4t+1)$th powers of β in the rows of the parity check matrix means that if $\epsilon \in \{\pm 1, \pm i\}$ then $\epsilon^{4t+1} = \epsilon$. If $\boldsymbol{c} = (c_0, c_1, \cdots, c_{n-1})$ is a codeword of $\mathcal{C}$ then—written as a polynomial $\boldsymbol{c} = c(x) = \sum c_j x^j$—we get

$$c(\beta^{4k+1}) = 0, \quad \text{for } k = 0, 1, \cdots, t.$$

Thus, we see that $c(x)$ is multiple of a generator polynomial $g(x)$ which divides $x^n - i$. Hence, $\mathcal{C}$ is an icyclic code, i.e., if

$$\begin{aligned} c(x) \in \mathcal{C} \Rightarrow x \cdot c(x) - c_{n-1} \cdot (x^n - i) \\ = (i \cdot c_{n-1}, c_0, c_1, \cdots, c_{n-2}) \in \mathcal{C}. \end{aligned}$$

Thus, multiplying $c(x)$ by x modulo $x^n - i$ means the following.

- Shifting the codeword by one position as for cyclic codes.
- The highest coefficient c_{n-1} is rotated by 90° in the complex plane and becomes c_0.

Remark: If $\beta^n = -i$ we get nega-icyclic codes.

The check polynomial $h(x)$ is defined by

$$x^n - i = g(x) \cdot h(x). \qquad (14)$$

Definition 2: Icyclic (nega-icyclic) codes over $\mathcal{G}_{\pi^r}$ are codes whose codewords are multiples of a generator polynomial $g(x)$ which divides $x^n - i$ (resp., $x^n + i$). Thus, icyclic codes belong to the class of constacyclic codes.

To determine the true minimum Mannheim distance of icyclic codes (or nega-icyclic codes) defined above seems to be a difficult problem, we therefore consider only the most simple cases. $t = 0$ gives OMEC codes, so let us treat the case $t = 1$ in more detail and consider whether the following parity-check matrix $\boldsymbol{H}$ can handle Mannheim errors of weight two.

$$\boldsymbol{H} = \begin{pmatrix} \beta^0, & \beta^1, & \beta^2, & \cdots, & \beta^{n-1} \\ \beta^0, & \beta^5, & \beta^{10}, & \cdots, & \beta^{(n-1)\cdot 5} \end{pmatrix}. \qquad (15)$$

Let $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e}$ be a received vector. First we compute the syndrome $\boldsymbol{s}$:

$$s = \begin{pmatrix} s_1 \\ s_5 \end{pmatrix} = \boldsymbol{H} \cdot \boldsymbol{r}^{\mathrm{T}}.$$

Suppose that at positions $l_{1,2}$ we have Mannheim errors with values $\beta^{L_{1,2} - l_{1,2}} \in \{\pm 1, \pm i\}$, then we try to compute the error determinator polynomial $\sigma(z)$.

$$\begin{aligned} \sigma(z) &= (z - \beta^{L_1}) \cdot (z - \beta^{L_2}) \\ &= z^2 - (\beta^{L_1} + \beta^{L_2}) z + \beta^{L_1} \cdot \beta^{L_2} \\ \Rightarrow \sigma(z) &= z^2 - s_1 z + \xi \end{aligned}$$

with ξ to be determined from the syndromes. We call $\sigma(z)$ error determinator polynomial rather than error locator polynomial, as knowledge of $\beta^{L_{1,2}}$ determines both the locations $l_{1,2} = L_{1,2} \bmod n$ and the values $\beta^{L_{1,2} - l_{1,2}}$ of the errors. From $s_1 = \beta^{L_1} + \beta^{L_2}$, $s_5 = \beta^{5L_1} + \beta^{5L_2}$, and $\xi = \beta^{L_1 + L_2}$ we get

$$\begin{aligned} \frac{s_1^5 - s_5}{5 s_1} &= (\beta^{L_1 + 4L_2} + 2\beta^{2L_1 + 3L_2} + 2\beta^{3L_1 + 2L_2} + \beta^{4L_1 + L_2}) / \\ &\quad (\beta^{L_1} + \beta^{L_2}) \\ &= (\xi \cdot \beta^{3L_2} + 2\xi^2 \cdot \beta^{L_2} + 2\xi^2 \cdot \beta^{L_1} + \xi \cdot \beta^{3L_1}) / \\ &\quad (\beta^{L_1} + \beta^{L_2}) \\ &= \xi \cdot \frac{\beta^{3L_2} + \beta^{3L_1}}{\beta^{L_1} + \beta^{L_2}} + 2 \cdot \xi^2 \\ &= \xi \cdot (\beta^{2L_2} - \beta^{L_1 + L_2} + \beta^{2L_1}) + 2 \cdot \xi^2 \\ &= \xi \cdot (s_1^2 - 3 \cdot \xi) + 2 \cdot \xi^2 \end{aligned}$$

from which we obtain the quadratic

$$\xi^2 - s_1^2 \cdot \xi + \frac{s_1^5 - s_5}{5 \cdot s_1} = 0.$$

Thus,

$$\xi_{1,2} = \frac{s_1^2}{2} \cdot \left(1 \pm \sqrt{\frac{s_1^5 + 4 s_5}{5 \cdot s_1^5}} \right).$$

Putting this into the error determinator polynomial leads to either

$$z_{1,2} = \frac{s_1}{2} \cdot \left(1 \pm \sqrt{-1 - 2 \cdot \sqrt{\frac{s_1^5 + 4 s_5}{5 \cdot s_1^5}}} \right)$$

or

$$z_{1,2} = \frac{s_1}{2} \cdot \left(1 \pm \sqrt{-1 + 2 \cdot \sqrt{\frac{s_1^5 + 4 s_5}{5 \cdot s_1^5}}} \right).$$

Hence, there is an ambiguity which indicates that the code defined by the parity check matrix of (15) in general cannot correct errors of Mannheim weight two. However, examples of codes which can be decoded by the above formulas are contained in Table X (the codes with $d_M \geq 5$). The above formulas are also useful for soft-decision decoders (see, e.g., [2, p. 237]). As the OMEC codes of the previous section contain the above codes we clearly have $d_M \geq 3$. In fact, the minimum distance can be as low as three as the following example shows.

Example 3: Let $p = 13$, $r = 1$, $n = 3$, $\alpha = 1 + i$ then using Table II we get

$$g(x) = (x - \alpha) \cdot (x - \alpha^5) = x^2 + i \cdot x - 1.$$

Hence, we see that $d_M = 3$ and $g(x)$ defines a [3, 1, 3] code.

We now consider cases where (15) leads to higher Mannheim distance. The first is given by the following theorem.

Theorem 1: For $p \equiv 5 \bmod 12$ and $n = (p-1)/4$ the code defined by (15) has $d_M \geq 4$.

Proof: We show that the decoder can distinguish single and double errors. Assume that an error of Mannheim weight one did occur. Then $s_1^5 = s_5 \neq 0$ and we get either

$$z_{1,2} = \begin{cases} 0 \\ s_1 \end{cases}$$

or

$$z_{3,4} = \frac{s_1}{2}(1 \pm \sqrt{-3}).$$

The case $z_1 = 0$ can be excluded and $z_2 = s_1$ leads to the correct error. For $p \equiv 5 \bmod 12$ Gauss's reciprocity law tells us that -3 is a quadratic non-residue of p, hence, $z_{3,4} \notin \mathcal{G}_\pi$. Thus, we can distinguish between single and double errors and the theorem follows.

For illustration consider the following example.

Example 4: For $p = 17$, $r = 1$, $n = 4$, using $\alpha = 1 + i$ the generator polynomial $g(x) = (x - \alpha) \cdot (x - \alpha^5)$ (see Table III) gives a [4, 2, 4] code having the following weight distribution:

$$A(z) = 1 + 16 \cdot z^4 + 16 \cdot z^5 + 32 \cdot z^6 + 64 \cdot z^7 + 80 \cdot z^8 + 64 \cdot z^9 + 16 \cdot z^{11}.$$

The codewords of weight 4 are the icyclic shifts of the codeword $c = (i, -1, 2, 0)$, and the codewords of weight 5 the icyclic shifts of $(2i, -2, -i, 0)$. Hence, the coding gain of this code on a Gaussian channel at high signal-to-noise ratio is

$$G = 10 \cdot \log_{10} \left(\frac{2}{4}(2^2 + 2 \cdot 1^2) \right) \approx 4.77 \text{ dB}.$$

Another simple way to get some good short $[n, n-2, d_M > 4]$ codes is by shortening codes generated by $g(x) = (x - \beta)(x - \beta^5)$.

Example 5: Let $\pi = 5 + 2i$, $\alpha = 2$ and $g(x) = (x - \alpha) \cdot (x - \alpha^5)$. By Theorem 1, $g(x)$ generates a [7, 5, 4] code. If we only consider codewords $c(x) = i(x) \cdot g(x)$ of degree smaller than five we get a [5, 3, 5] code which has the following weight distribution:

$$\begin{aligned} A(z) = 1 &+ 28z^5 + 100z^6 + 264z^7 + 548z^8 + 1020z^9 \\ &+ 1716z^{10} + 2680z^{11} + 3376z^{12} + 3684z^{13} + 3592z^{14} \\ &+ 3128z^{15} + 2200z^{16} + 1240z^{17} + 568z^{18} \\ &+ 208z^{19} + 36z^{20}. \end{aligned}$$

For further codes of this kind see Table X. Theorem 1 gives a bound on d_M which does not depend on a particular primitive element α. In general, however, the true minimum Mannheim distance depends very much on the chosen α (or $4n$th root β), e.g., taking $\alpha = 2 + 2i$ in the example above only leads to a [5, 3, 4] code.

We now give a list of $[2, 1, d_x]$ codes found with the help of a computer. The construction is as follows. Let $m \in \mathcal{G}_\pi$ then the code $\mathcal{C}$ consists of all polynomials $m \cdot (x + \delta)$, i.e., the codewords $\boldsymbol{c} = (m, \delta \cdot m)$ with δ chosen such that the minimum Mannheim distance is as high as possible. Tables XI–XII give the parameters of $[2, 1, d_x]$ codes constructed in this way. Note that the coding gain $G = 10 \log_{10} (d_E^2/2)$ of these codes is much higher than $10 \log_{10} (d_M/2)$ because of the short length $n = 2$. (Among the possible δ's which give the highest Mannheim distance d_x, δ has been selected such that the coding gain is maximal.) For $d_x \gg 1$ the gain G can be approximated by

$$G \approx 10 \cdot \log_{10} \frac{1}{2} \left(3 \left\lfloor \frac{d_x}{4} \right\rfloor^2 + \left\lceil \frac{d_x}{4} \right\rceil^2 \right) \text{ dB} \approx 10 \cdot \log_{10} \frac{d_x^2}{2} \text{ dB}.$$

Decoding of these codes is fairly straightforward. If $\boldsymbol{r} = \boldsymbol{c} + \boldsymbol{e} = (r_1, r_2) = (m + e_1, \delta m + e_2)$ is received, simply compute $(r_1 + t, \delta \cdot (r_1 + t))$ and/or $(\delta^{-1} \cdot (r_2 + t), r_2 + t)$ for all t of low Mannheim weight until the closest codeword is found.

Using the $[2, 1, d_x]$ codes together with a $[N, K, D_H]$ Hamming error correcting code over $GF(p)$ we can easily construct $[2N, K, D_H \cdot d_x]$ Mannheim error correcting codes as follows. Let $c_H = (c_0, c_1, \cdots, c_{N-1})$ be a codeword of the $[N, K, D_H]$ code then the construction

$$c_M = (\mu(c_0), \delta \cdot \mu(c_0), \mu(c_1), \delta \cdot \mu(c_1), \cdots, \cdot\mu(c_{N-1}), \delta \cdot \mu(c_{N-1})) \quad (16)$$

clearly gives the codewords of a $[2N, K, D_H \cdot d_x]$ code.

Example 6: Take the $[40, 27, D_H = 14]$ RS code over $GF(41)$ and the $[2, 1, d_x = 4]$ code from Table XI to get a $[80, 27, d_M = 56]$ code over $\mathcal{G}_{5+i4}$ which reaches a coding gain of $G = 10 \cdot \log_{10} (27 \cdot 14/40) + 5.44$ dB ≈ 14.9 dB (this is a gain of about 7.8 dB over BPSK, see Table XIV).

In the same way $[n, n-r, d_M = 3]$ OMEC codes can be used as inner codes leading to $[N \cdot n, K \cdot (n-r), D_H \cdot d_M]$ Mannheim error correcting codes.

Example 7: Again take the $[40, 27, D_H = 14]$ RS code over $GF(41)$ and the [10, 9, 3] OMEC code over $\mathcal{G}_{5+i4}$ to get a [400, 243, 42] code over $\mathcal{G}_{5+i4}$ which leads to a coding gain of

$$\begin{aligned} G &= 10 \cdot \log_{10} \left(\frac{27}{40} \cdot \frac{9}{10} \cdot 42 \right) \text{ dB} \\ &\approx 14.07 \text{ dB (about 7 dB over BPSK see Table XIV)} \end{aligned}$$

To finish this section let us comment on a practical aspect. Usually data are organized in bits and bytes, hence primes like $p = 41$ are not particularly pleasing. There are two straightforward ways to handle this problem. The first is to group a convenient number of bits or bytes together such that the number representable by these bits is close to a power of p. (For example, two bytes can be efficiently represented by three symbols from $GF(41)$ as $2^{16}/41^3 \approx 0.95 < 1$). Thus, the nonprimitive icyclic [5, 3, 6] code of Table X can be used to encode two bytes of information. Note also that primes of the form $p = (b+1)^2 + b^2$ give particularly nice square QAM signal constellations (the parameters of $[2, 1, d_x]$ codes for the first square QAM primes are given in Table XII).

Another way is to consider nonlinear subcodes of the codes presented. We will explain this by a small example. The signal constellation of $\mathcal{G}_{5+i\cdot 4}$ (see Fig. 6) contains the 16 QAM signal constellation as a subset (namely, the points $\{\pm 1, \pm 3, \pm i, \pm 3i, \pm(1 \pm 2i), \pm(2 \pm i)\}$). We now encode in a systematic way, i.e., the information can be read directly in the codeword. Hence the coefficients of the information part can now be chosen from the 16-QAM subset of $\mathcal{G}_{5+i4}$. Doing this costs about $-10 \log_{10} (4/\log_2 (41)) \approx 1.27$ dB. For example the nonlinear subcode of Example 7 would give a coding gain of about 12.8 dB. On the other hand using a nonlinear subcode gives an extra error detection capability and can help in improving the decoding error probability. (In a concatenation scheme this can, e.g., be used to set erasures.) In the same way 64 or 256 QAM constellations can be encoded. For illustration consider the following example:

Example 8: Take the [2, 1, 5] code of Table XI and a [112, 75, 38] RS code over $GF(113)$. Using the 64 QAM subset of $\mathcal{G}_{8+i\cdot 7}$ in the information part of the codeword leads to a nonlinear code of length 224, having $2^{6\cdot 75}$ codewords and minimum Mannheim distance 190. The coding gain of this code is about $10 \log_{10} (75 \cdot 38/112) + 7.4 + 10 \log_{10} (6/\log_2 113)$ dB ≈ 20.9 dB. For comparison, the linear [224, 75, 190] code over $\mathcal{G}_{8+i7}$ would give a gain of ≈ 21.5 dB.

Using small subsets of large fields $\mathcal{G}_\pi$ also gives an algebraic approach for soft-decision block coding once efficient decoders of e Mannheim error correcting codes are available.

V. Extension for Primes $p \equiv 3 \bmod 4$

For primes $p \equiv 3 \bmod 4$ the number -1 is a quadratic nonresidue of p. Hence, we immediately get an isomorphism between $GF(p^2)$ and $\mathcal{G}_{ip}$ where

$$\mathcal{G}_{ip} = \{k + i \cdot l | k, \, l \in \{-(p-1)/2, \cdots -1, \, 0, \, 1, \cdots, (p-1)/2\}\},$$

by constructing $GF(p^2)$ using the irreducible polynomial x^2+1. As an example the set $\mathcal{G}_{i3}$ is visualised in Fig. 7. In this way the results of the previous sections can be extended simply by replacing $p \rightarrow p^2$.

Example 9: Using $\delta = 1 + i$, the $\boldsymbol{c} = (m, \, \delta \cdot m)$ construction leads to a [2, 1, 3] code over $GF(3^2)$ which is identical to the perfect icyclic OMEC code. The gain of this code is $G \approx 1.76$ dB.

In the same way $\delta = 2 + i \cdot 2$ leads to a [2, 1, 5] code over $GF(7^2)$ and $\delta = 2 + i \cdot 3$ to a [2, 1, 6] code over $GF(11^2)$ having gains of 6.53 dB and 8.13 dB, respectively.

VI. Conclusion and Suggestions for Further Research

It has been shown how a new two-dimensional modular distance called Mannheim distance can be used for the construction of efficient block codes for QAM signal constellations. The focus of this paper has been on channel coding, although other applications are conceivable. The Mannheim distance is much better suited for coding over two dimensional signal space than the Hamming distance, as it—in a sense—approximates the Euclidean distance, which means that vectors which are close according to the Euclidean metric are also close according to the Mannheim metric (ignoring quantization effects). The Mannheim metric allows an algebraic approach in an area which is nowadays mainly dominated by nonalgebraic convolutional codes. Also the codes presented here are 90° rotationally invariant, which is very useful in communications. This paper also gives rise to many research problems including the following.

1) The determination of all perfect Mannheim error correcting codes.

2) The development of tight bounds for Mannheim error correcting codes.

3) The determination of the true minimum Mannheim distance of icyclic Mannheim error correcting codes.

4) The development of an efficient decoding algorithm for e-Mannheim error correcting icyclic codes, which will enable algebraic soft decision decoding of block codes.

5) The determination of the minimum Mannheim distance of t-error correcting BCH- and RS-codes (or other well-known classes of codes).

6) The use of the Mannheim distance for sphere packing.

Appendix A
Signal Constellations Obtained from $p = 5$, 13, 17, 29, 37, 41

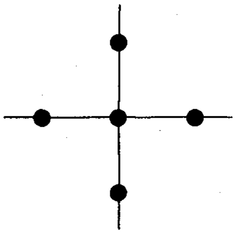

Fig. 1. $\mathcal{G}_{2+i}$.

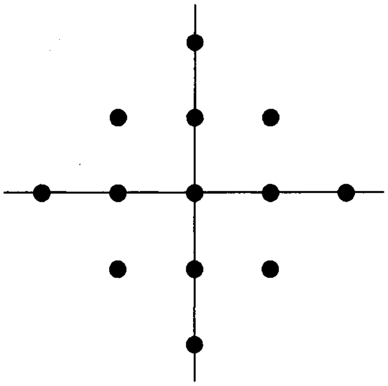

Fig. 2. $\mathcal{G}_{3+i \cdot 2}$.

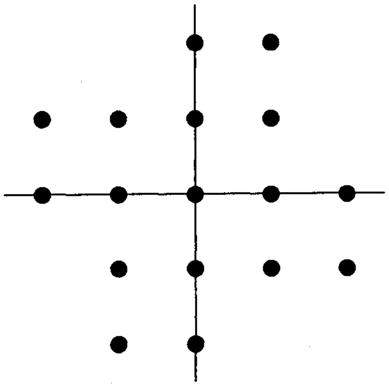

Fig. 3. $\mathcal{G}_{4+i}$.

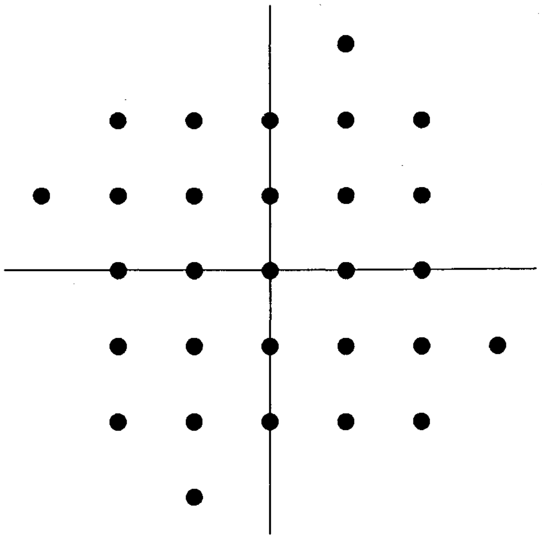

Fig. 4. $\mathcal{G}_{5+i \cdot 2}$.

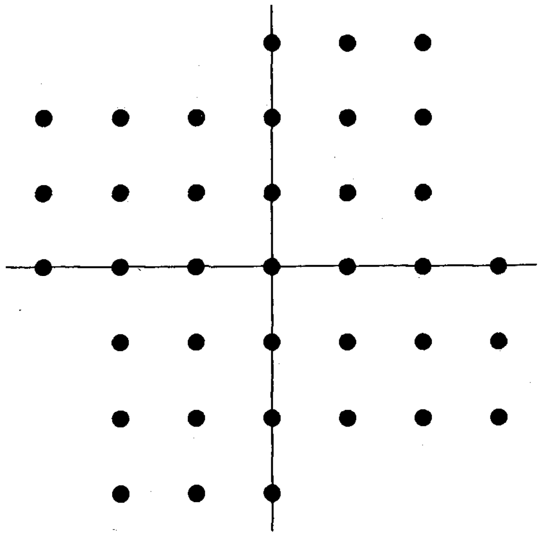

Fig. 5. $\mathcal{G}_{6+i}$.

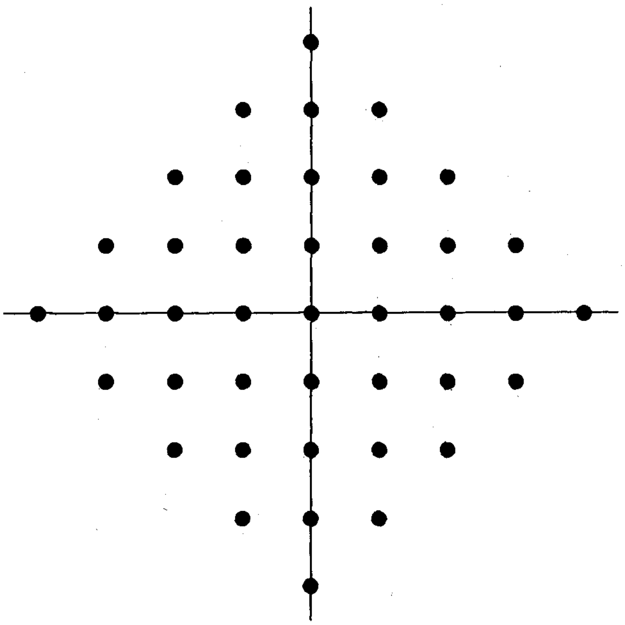

Fig. 6. $\mathcal{G}_{5+i\cdot 4}$.

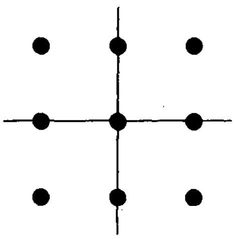

Fig. 7. $\mathcal{G}_{i3}$.

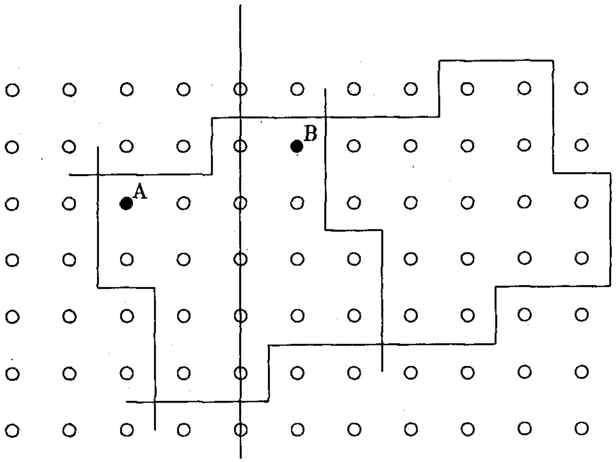

Fig. 8. The Manhattan distance between $A = -2 + i$ and $B = 1 + 2i$ equals 4. The Mannheim distance $\bmod 4 + i$ between A and B equals 1, as $-2 + i \equiv 2 + 2i \bmod 4 + i$.

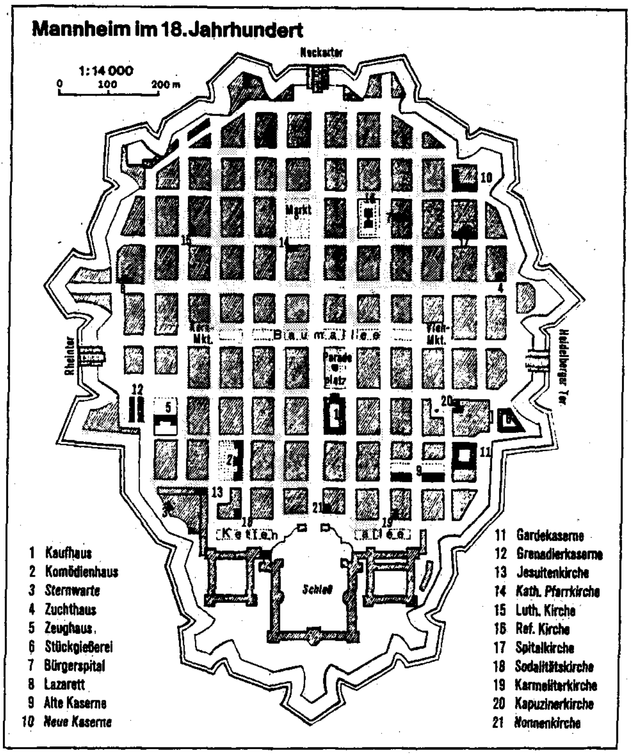

Fig. 9. Street map of Mannheim.

APPENDIX B
EXPONENT TABLES OF $\mathcal{G}_{\pi^r}$ FOR SOME SMALL FIELDS

TABLE I
$\mathcal{G}_{2+i}$

s	α^s	s	α^s	s	α^s	s	α^s
0	1	1	i	2	-1	3	$-i$

TABLE II
$\mathcal{G}_{3+i\cdot 2}$

s	α^s	s	α^s	s	α^s	s	α^s
0	1	3	$-i$	6	-1	9	i
1	$1+i$	4	$1-i$	7	$-1-i$	10	$-1+i$
2	$i\cdot 2$	5	2	8	$-i\cdot 2$	11	-2

TABLE III
$\mathcal{G}_{4+i}$

s	α^s	s	α^s	s	α^s	s	α^s
0	1	4	i	8	-1	12	$-i$
1	$1+i$	5	$-1+i$	9	$-1-i$	13	$1-i$
2	$i\cdot 2$	6	-2	10	$-i\cdot 2$	14	2
3	$-1-i\cdot 2$	7	$2-i$	11	$1+i\cdot 2$	15	$-2+i$

[redacted]

TABLE IV
$\mathcal{G}_{5+i\cdot 2}$

[redacted]	α^s	[redacted]	[redacted]	[redacted]	α^s	s	α^s
[redacted]	1	7	[redacted]	14	-1	21	i
[redacted]	$2+i\cdot 2$	8	[redacted]	15	$-2-i\cdot 2$	22	$-2+i\cdot 2$
[redacted]	$-3+i$	9	[redacted]	16	$3-i$	23	$-1-i\cdot 3$
[redacted]	2	10	[redacted]	17	-2	24	$i\cdot 2$
[redacted]	[redacted]	11	[redacted]	18	$1-i\cdot 2$	25	$-2-i$
[redacted]	$1-i$	12	[redacted]	19	$-1+i$	26	$1+i$
[redacted]	[redacted]	13	[redacted]	20	$1+i\cdot 2$	27	$2-i$

TABLE V
$\mathcal{G}_{6+i}$

s	α^s	s	α^s	s	α^s	s	α^s
0	1	9	i	18	-1	27	$-i$
1	$1+i$	10	$-1+i$	19	$-1-i$	28	$1-i$
2	$i\cdot 2$	11	-2	20	$-i\cdot 2$	29	2
3	$-2+i\cdot 2$	12	$-2-i\cdot 2$	21	$2-i\cdot 2$	30	$2+i\cdot 2$
4	$2+i$	13	$-1+i\cdot 2$	22	$-2-i$	31	$1-i\cdot 2$
5	$1+i\cdot 3$	14	$-3+i$	23	$-1-i\cdot 3$	32	$3-i$
6	$-1-i\cdot 2$	15	$2-i$	24	$1+i\cdot 2$	33	$-2+i$
7	$i\cdot 3$	16	-3	25	$-i\cdot 3$	34	3
8	$-2-i\cdot 3$	17	$3-i\cdot 2$	26	$2+i\cdot 3$	35	$-3+i\cdot 2$

TABLE VI
$\mathcal{G}_{5+i\cdot 4}$

s	α^s	s	α^s	s	α^s	s	α^s
0	1	10	i	20	-1	30	$-i\cdot 1$
1	$-1-i\cdot 3$	11	$3-i$	21	$1+i\cdot 3$	31	$-3+i$
2	$-i\cdot 4$	12	4	22	$i\cdot 4$	32	-4
3	$1-i\cdot 2$	13	$2+i$	23	$-1+i\cdot 2$	33	$-2-i$
4	$2-i\cdot 2$	14	$2+i\cdot 2$	24	$-2+i\cdot 2$	34	$-2-i\cdot 2$
5	-3	15	$-i\cdot 3$	25	3	35	$i\cdot 3$
6	2	16	$i\cdot 2$	26	-2	36	$-i\cdot 2$
7	$-1+i\cdot 3$	17	$-3-i$	27	$1-i\cdot 3$	37	$3+i$
8	$1+i$	18	$-1+i$	28	$-1-i\cdot 1$	38	$1-i$
9	$-2+i$	19	$-1-i\cdot 2$	29	$2-i\cdot 1$	39	$1+i\cdot 2$

TABLE VII
$\mathcal{G}_{(2+i)^2}$ CONSTRUCTED USING α WHICH IS ROOT OF $p(x) = x^2 + x - i$

s	α^s	s	α^s	s	α^s	s	α
0	$(0,1)$	6	$(0,-i)$	12	$(0,-1)$	18	$(0,i)$
1	$(1,0)$	7	$(-i,0)$	13	$(-1,0)$	19	$(i,0)$
2	$(-1,i)$	8	$(i,1)$	14	$(1,-i)$	20	$(-i,-1)$
3	$(1+i,-i)$	9	$(1-i,-1)$	15	$(-1-i,i)$	21	$(-1+i,1)$
4	$(1-i,-1+i)$	10	$(-1-i,1+i)$	16	$(-1+i,1-i)$	22	$(1+i,-1-i)$
5	$(-1,1+i)$	11	$(i,1-i)$	17	$(1,-1-i)$	23	$(-i,-1+i)$

APPENDIX C
TABLE OF p, π, α, $d_{\max}$, u AND v FOR $p \leq 113$

TABLE VIII
TABLE OF p, π, A PRIMITIVE α, $d_{\max}$, u AND v (WHERE $1 = u \cdot \pi + v \cdot \pi^*$) FOR $p \leq 113$

p	π	α	d_{max}	u,	v
5	$2+i$	$-i$	1	-1 ,	$1+i$
13	$3+i2$	2	2	-2 ,	$1+i2$
17	$4+i$	$-1-i$	3	-2 ,	$2+i$
29	$5+i2$	2	4	$-2+i2$,	3
37	$6+i$	2	5	-3 ,	$3+i$
41	$5+i4$	$-3+i$	4	-4 ,	$1+i4$
53	$7+i2$	2	6	$-4-i$,	$3+i3$
61	$6+i5$	2	5	$i6$,	$6-i$
73	$8+i3$	$-3-i3$	7	$-3+i4$,	$5-i$
89	$8+i5$	3	7	$-3+i4$,	$5+i$
97	$9+i4$	5	8	$-4+i3$,	$5+i$
101	$10+i$	2	9	-5 ,	$5+i$
109	$10+i3$	$-4-i3$	9	$-3+i8$,	$7-i5$
113	$8+i7$	3	7	$i8$,	$8-i$

APPENDIX D
PERFORMANCE OF CERTAIN MANNHEIM ERROR CORRECTING CODES

Table IX gives $G_{\max}$, the maximum asymptotic coding gain for code rate $R \rightarrow 1$ on a Gaussian channel by using Mannheim error correcting codes. Clearly, for any p we have Euclidean distance $d_E \geq \sqrt{d_M}$, hence $G_{\max} \approx 10 \cdot \log_{10}(d_M)$ dB.

TABLE IX
ASYMPTOTIC CODING GAIN FOR MANNHEIM ERROR CORRECTING CODES

d_M	3	4	5	6	7	8	9	10	11	12	13
$d_E \geq$	$\sqrt{3}$	$\sqrt{4}$	$\sqrt{5}$	$\sqrt{6}$	$\sqrt{7}$	$\sqrt{8}$	$\sqrt{9}$	$\sqrt{10}$	$\sqrt{11}$	$\sqrt{12}$	$\sqrt{13}$
G_{max}/dB	4.77	6.02	6.99	7.78	8.45	9.03	9.54	10.0	10.4	10.8	11.1

Note, that for short length n the true minimum Euclidean distance d_E of the codes can be higher than $\sqrt{d_M}$, leading to a higher coding gain. The following table gives the gain $G = 10 \cdot \log_{10}(R \cdot d_E^2)$ for some short codes. Among them are codes which have $d_E > \sqrt{d_M}$. The column "primitive" indicates whether the root β_1 of $g(x)$ is a primitive element of $\mathcal{G}_\pi$. The roots of $g(x) = (x - \beta_1) \cdot (x - \beta_1^5)$ are given in the column of β_1, β_2.

The following table lists the few $[2, 1, d_x]$ codes which have lower minimum Mannheim distance, but give higher coding gain than the corresponding codes of Tables XI and XII.

To be able to compare the coding gain of the codes given with the common BPSK or QPSK modulation, Table XIV gives some data about the signal energy per symbol E_s, the energy per bit $E_b = E_s/\log_2 p$ and the BPSK/QPSK reference $10 \cdot \log_{10}(4E_b)$. This value must be subtracted from the coding gain to obtain the improvement over BPSK or QPSK (see Examples 6, 7).

APPENDIX E
PROPERTIES OF GAUSSIAN INTEGERS

For convenience well-known properties of Gaussian integers as needed for this paper are given. For proofs and details see, e.g., [3]. The Gaussian integers are those complex numbers which have

TABLE X
CODING GAIN FOR SOME CODES GENERATED BY $g(x) = (x - \beta_1)(x - \beta_1^5)$

p	$[n,k,d_M]$	G	primitive	β_1	β_2
13	[3,1,4]	2.22 dB	no	$-i$	$-i$
17	[4,2,4]	4.77 dB	yes	$1+i$	$-1+i$
	[3,1,4]	3.01 dB	yes	$1+i$	$-1+i$
29	[7,5,4]	4.56 dB	yes	2	$-2-i2$
	[6,4,4]	4.26 dB	yes	2	$-2-i2$
	[5,3,5]	4.77 dB	yes	2	$-2-i2$
	[4,2,5]	3.98 dB	yes	2	$-2-i2$
	[3,1,7]	5.64 dB	no	$-1-2i$	$-3+i$
37	[9,7,4]	4.93 dB	yes	2	$1+i$
	[8,6,4]	4.77 dB	yes	2	$1+i$
	[7,5,4]	4.56 dB	yes	2	$1+i$
	[6,4,4]	4.26 dB	yes	2	$1+i$
	[5,3,5]	4.77 dB	yes	2	$1+i$
	[4,2,5]	3.98 dB	yes	2	$1+i$
	[3,1,7]	5.64 dB	yes	2	$1+i$
41	[10,9,3]	4.31 dB	yes	$-1-3i$	-3
	[10,8,4]	5.05 dB	yes	$-1-3i$	-3
	[5,3,6]	5.56 dB	no	$-4i$	i
	[5,3,4]	5.56 dB	yes	$-1-3i$	-3
	[4,2,6]	4.77 dB	no	$-4i$	i
	[4,2,5]	5.44 dB	yes	$1-2i$	$-3i$
	[3,1,5]	3.68 dB	yes	$-1-3i$	-3
	[3,1,6]	4.26 dB	no	$-4i$	i

TABLE XI
TABLE OF $[2,\ 1,\ d_x]$ CODES WITH CONSTRUCTION $c = (m,\ \delta \cdot m)$

p	π	δ	d_x	G
5	$2+i$	$-i$	2	0.00 dB
13	$3+i2$	2	3	1.76 dB
17	$4+i$	$i2$	3	3.98 dB
29	$5+i2$	$-1-i2$	4	4.77 dB
37	$6+i$	$-2-i$	4	4.77 dB
41	$5+i4$	$i3$	4	5.44 dB
53	$7+i2$	$-3-i2$	5	5.44 dB
61	$6+i5$	4	5	5.44 dB
73	$8+i3$	$-2-i2$	5	6.53 dB
89	$8+i5$	$3+i$	5	7.40 dB
97	$9+i4$	$-2+i3$	5	8.13 dB
101	$10+i$	$-3-i$	5	7.40 dB
109	$10+i3$	$-2+i3$	5	7.40 dB
113	$8+i7$	$-3+i2$	5	7.40 dB
137	$11+i4$	$-4-i5$	6	8.13 dB
149	$10+i7$	$-2+i6$	6	8.45 dB
157	$11+i6$	$-2-i3$	6	8.45 dB
173	$13+i2$	$-5+i5$	7	8.75 dB
181	$10+i9$	$-1+i4$	6	8.75 dB
193	$12+i7$	-8	7	9.29 dB
197	$14+i$	$4-i2$	7	9.54 dB
229	$15+i2$	$-7-i3$	7	9.54 dB
233	$13+i8$	$1+i8$	7	9.78 dB
241	$15+i4$	$-i8$	7	10.21 dB
257	$16+i$	$2+i8$	7	9.54 dB
269	$13+i10$	$-3-i3$	7	9.78 dB
277	$14+i9$	$-3-i8$	7	10.21 dB
281	$16+i5$	$-2+i4$	7	10.21 dB
293	$17+i2$	$8-i5$	7	9.78 dB
313	$13+i12$	$-9-i$	7	10.21 dB
317	$14+i11$	$2+i9$	7	10.21 dB
337	$16+i9$	$-7+i3$	8	9.54 dB
349	$18+i5$	$-6+i8$	8	10.41 dB
353	$17+i8$	$-7-i$	8	10.21 dB
373	$18+i7$	$4+i7$	8	10.61 dB
389	$17+i10$	$-2+i5$	8	11.14 dB
397	$19+i6$	$5-i4$	8	10.41 dB

TABLE XII
TABLE OF SQUARE QAM $[2,\ 1,\ d_x]$ CODES WITH CONSTRUCTION $c = (m,\ \delta{\cdot}m)$

p	π	δ	d_x	G
5	$2+i$	$-i$	2	0.00 dB
13	$3+i2$	2	3	1.76 dB
41	$5+i4$	$i3$	4	5.44 dB
61	$6+i5$	4	5	5.44 dB
113	$8+i7$	$-3+i2$	5	7.40 dB
181	$10+i9$	$-1+i4$	6	8.75 dB
313	$13+i12$	$-9-i$	7	10.21 dB
421	$15+i14$	$-2+i5$	8	10.61 dB
613	$18+i17$	$6+i2$	9	11.76 dB
761	$20+i19$	$-6-i13$	9	11.90 dB
1013	$23+i22$	$-9-i6$	10	12.90 dB
1201	$25+i24$	$-20-i2$	11	13.22 dB
1301	$26+i25$	$21+i2$	11	13.12 dB
1741	$30+i29$	$2+i21$	12	13.98 dB
1861	$31+i30$	$-24-i6$	12	14.23 dB
2113	$33+i32$	$12-i$	13	14.23 dB
2381	$35+i34$	$-19-i13$	13	14.91 dB

TABLE XIII
TABLE OF $[2,\ 1,\ d_x]$ CODES WITH δ SELECTED FOR MAXIMAL GAIN G

p	π	δ	d_x	G
61	$6+i5$	3	4	6.53 dB
157	$11+i6$	$i4$	5	8.75 dB
337	$16+i9$	$3-i4$	7	10.97 dB
761	$20+i19$	$1+i6$	8	12.17 dB
1201	$25+i24$	$i7$	8	13.32 dB
1301	$26+i25$	-7	8	13.52 dB
1741	$30+i29$	$-1-i7$	9	14.07 dB
1861	$31+i30$	$26-i3$	11	14.31 dB
2113	$33+i32$	$-8-i$	10	14.58 dB

TABLE XIV
TABLE OF E_s, E_b AND $10\log_{10}(4E_b)$

p	π	E_s	E_b	$10\log 4E_b$
5	$2+i$	0.800	0.345	1.393 dB
13	$3+i2$	2.154	0.582	3.670 dB
17	$4+i$	2.824	0.691	4.414 dB
29	$5+i2$	4.828	0.994	5.993 dB
37	$6+i$	6.162	1.183	6.750 dB
41	$5+i4$	6.829	1.275	7.075 dB
53	$7+i2$	8.830	1.542	7.900 dB
61	$6+i5$	10.164	1.714	8.360 dB
73	$8+i3$	12.164	1.965	8.955 dB
89	$8+i5$	14.831	2.290	9.620 dB
97	$9+i4$	16.165	2.449	9.911 dB
101	$10+i$	16.832	2.528	10.048 dB
109	$10+i3$	18.165	2.684	10.308 dB
113	$8+i7$	18.832	2.761	10.432 dB
137	$11+i4$	22.832	3.217	11.095 dB
149	$10+i7$	24.832	3.440	11.386 dB
157	$11+i6$	26.166	3.587	11.568 dB
173	$13+i2$	28.832	3.878	11.907 dB
181	$10+i9$	30.166	4.022	12.065 dB
193	$12+i7$	32.166	4.237	12.291 dB
197	$14+i$	32.832	4.308	12.363 dB
229	$15+i2$	38.166	4.869	12.895 dB
233	$13+i8$	38.833	4.938	12.956 dB
241	$15+i4$	40.166	5.076	13.076 dB
257	$16+i$	42.833	5.350	13.304 dB
269	$13+i10$	44.833	5.554	13.467 dB
277	$14+i9$	46.166	5.690	13.572 dB
281	$16+i5$	46.833	5.757	13.623 dB
293	$17+i2$	48.833	5.959	13.772 dB
313	$13+i12$	52.166	6.293	14.009 dB
317	$14+i11$	52.833	6.359	14.054 dB
337	$16+i9$	56.166	6.689	14.274 dB
349	$18+i5$	58.166	6.886	14.400 dB
353	$17+i8$	58.833	6.951	14.441 dB
373	$18+i7$	62.166	7.277	14.640 dB
389	$17+i10$	64.833	7.536	14.792 dB
397	$19+i6$	66.166	7.664	14.865 dB

integers as real and imaginary parts. Let $\mathcal{G}$ be the set of all Gaussian integers. If $\gamma = g_1 + ig_2 \in \mathcal{G}$ where $i^2 = -1$, then $\gamma^* = g_1 - ig_2$ is called the *conjugate* of γ. The *norm* of a Gaussian integer $\gamma = g_1 + ig_2$ is defined by $N(\gamma) = g_1^2 + g_2^2 = \gamma \cdot \gamma^*$. There are 4 *unities*, i.e., elements of $\mathcal{G}$ which have norm 1, namely ± 1, $\pm i$. The elements $\pm\gamma$, $\pm i \cdot \gamma$ are called the *associates* of γ. The *Gaussian primes* are i) $1+i$ and its associates, ii) the rational primes p with $p \equiv 3 \bmod 4$ and their associates, and iii) the factors $a+ib$ of the rational primes p with $p \equiv 1 \bmod 4$. The expression of an integer as a product of Gaussian primes is unique, apart from the order of the primes, the presence of unities, and ambiguities between associated primes. Given any two integers γ, γ_1, of which $\gamma_1 \neq 0$, there is an integer κ such that $\gamma = \kappa\gamma_1 + \gamma_2$, with $N(\gamma_2) < N(\gamma_1)$. This permits an analogue of Euclid's algorithm for Gaussian integers.

Performing the Euclidean algorithm with Gaussian integers is almost as simple as with ordinary integers. For ordinary integers a version of the basic Euclidean sequence is $a = q \cdot b + r$ where $q = [a/b]$ and $[\cdot]$ denotes rounding to the closest integer. For Gaussian integers we can define a rounding operation as follows:

Rounding of Gaussian Integers: $[a + i \cdot b] = [a] + i \cdot [b]$. Thus, we get a Euclidean sequence $\alpha = \lambda \cdot \beta + \gamma$ where $\lambda = [\alpha \cdot \beta^* / (\beta\beta^*)]$ and $N(\gamma) < N(\beta)$ which permits the computation of the greatest common divisor between two Gaussian integers. Also similarly as for ordinary integers the extended Euclidean algorithm for computing $\gcd(\beta, \gamma) = r \cdot \beta + s \cdot \gamma$ works for Gaussian integers.

Appendix F
A Fast Algorithm for Finding $p = a^2 + b^2$

For completeness we give a known algorithm to find the representation of a prime $p \equiv 1 \bmod 4$ as sum of two squares. A detailed exposition of this algorithm can be found in [4]. To represent $p \equiv 1 \bmod 4$ as sum of two squares ($p = a^2 + b^2$), the algorithm is as follows.

1) Find x such that $x^2 \equiv -1 \bmod p$. (If q_{nr} is a quadratic nonresidue of p then $x \equiv q_{nr}^{(p-1)/4} \bmod p$.)

2) Apply the Euclidean algorithm to p and x; the first two remainders less than $\sqrt{p}$ are a and b.

For further details see, e.g., Wagons paper.

Acknowledgment

I would like to thank Dr. M. Dietrich, Dr. W. Henkel, and Dr. K. H. Hofmann for helpful comments. Also thanks go to one referee for helpful criticism. The detailed treatment of Gaussian integers in Appendix E has been supplied at the request of a referee and the coeditor.

References

[1] E. R. Berlekamp, *Algebraic Coding Theory.* Aegean Park Press, 1984.
[2] R. E. Blahut, *Digital Transmission of Information.* Reading, MA: Addison-Wesley, 1990.
[3] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers.* Oxford, 1979, 5th ed.
[4] S. Wagon, "The Euclidean algorithm strikes again," *Amer. Mathemat. Monthly*, vol. 97, no. 2, pp. 125–129, 1990.

A Finite Group of Complex Integers and Its Application to Differentially Coherent Detection of QAM Signals

Robert G. Egri and Frank A. Horrigan

***Abstract*— A finite multiplicative group of complex integers is constructed and its application to differential detection of 16 QAM signals is given. In this group the algebraic properties of regular complex multiplication, such as commutativity, associativity, and conjugation are preserved. The challenge in finding such a group lies in the requirements for the existence of multiplicative inverses for numbers that have magnitudes different from 1, and for maintaining associativity. The group properties are used to demodulate 16 QAM signals in a differentially coherent way.**

***Index Terms*—Algebraic groups, differentially coherent detection, QAM signals.**

I. Introduction

Differentially coherent detection of phase shift keyed (PSK) signals is a widely used technique based on delaying the received symbol and multiplying its complex conjugate with the current symbol. This operation effectively provides a carrier phase reference as long as the phase variation is negligible over the duration of a few symbols [1]. It thereby obviates coherent carrier phase recovery, although with performance penalty. Differentially coherent detection of phase shift keyed signals can be represented as the product of two unit magnitude complex numbers, each corresponding to a symbol. The product is a member of the signal set and represents some other symbol. In other words, the symbol multiplications in the abstract signal space corresponds to multiplications of complex numbers. Of course, these complex numbers are all of unit magnitudes, and multiplication does not lead out of the signal set if the phases form an arithmetic progression, with one phase being fixed to zero. In algebraic language, the PSK symbols form a group with a one-to-one mapping to the complex roots of unity.

In contrast with phase shift keyed signals nonconstant amplitude QAM waveforms are always demodulated using phase coherent techniques. All coherent carrier phase recovery techniques suffer from phase ambiguities that are resolved by either a special encoding of the data symbols, or by recovering the absolute phase of the carrier through a unique word following the carrier acquisition. While it causes some loss in performance the former method is normally preferred for its simplicity. In fact, certain trellis codes are designed [5] to be rotationally invariant to remove the phase ambiguity of the recovered carrier. In either case, the carrier recovery complicates the hardware, and a differentially coherent demodulation would be an attractive alternative if its reduced noise immunity could be tolerated.

Differentially coherent detection can be generalized to amplitude modulated signals if a mapping and a group over a finite set of complex numbers can be found such that the properties of multiplication over the numbers is preserved as a group operation.

The challenge in finding such group lies in the requirements for the existence of multiplicative inverses for numbers that have magnitudes different from 1, and for maintaining associativity. Below we will

Manuscript received April 9, 1992; revised October 11, 1992.
R. G. Egri is with M/A-COM Inc., Lowell, MA 01853.
F. A. Horrigan is with Raytheon Research, Lexington, MA 02173.
IEEE Log Number 9215197.