Codierung von QAM-Signalen

Dr.-Ing. Klaus Huber
Sesenheimer Str. 21
10627 Berlin

Hochschule der Bayerischen Wirtschaft
07.05.2014

- Übersicht

- Kanalkapazität

- Blockcodes

- QAM Modulation

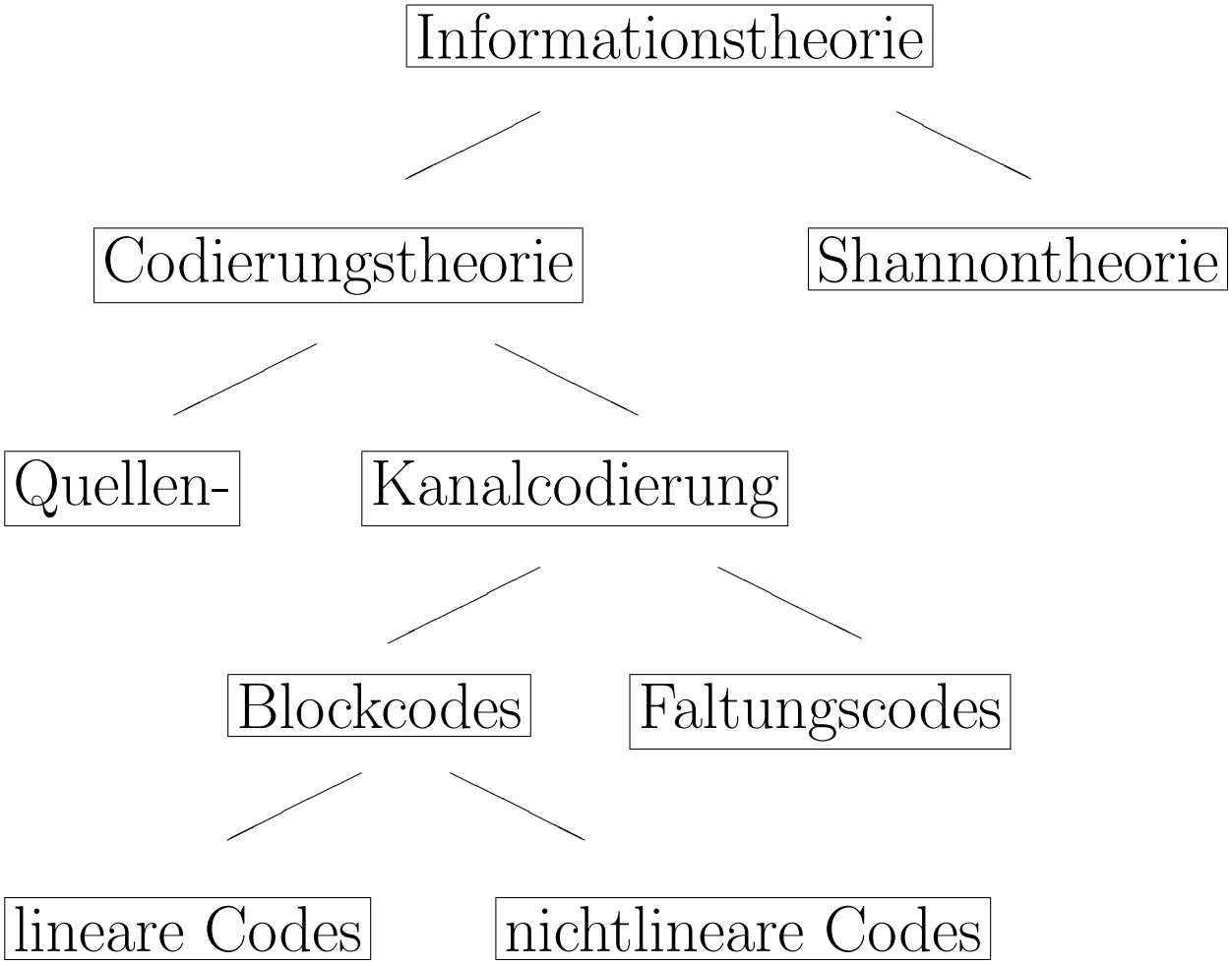
- Fermats Zwei Quadrate Satz

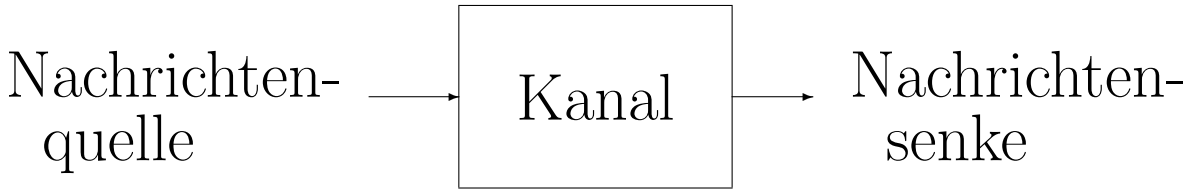
- Mannheim Distanz

- izyklische Codes

Übersicht

wissenschaftliche Basis der Informationstechnik:





Kanalkapazität C:
Gibt an mit welcher Datenrate prinzipiell
Nachrichten fehlerfrei übertragen werden können

Gängigste Kanäle:
Binärer symmetrischer Kanal

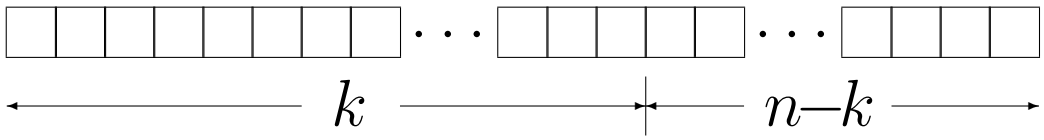
$$C = 1 + p\,\mathrm{ld}p + (1-p)\,\mathrm{ld}(1-p)$$

AWGN Kanal

$$C = W \log(1 + \frac{S}{N})$$

Blockcode $\mathcal{C}$: Menge von Codewörtern.

Codewort: Vektor mit n Zeichen



Zu k Informationszeichen aus einem Alphabet werden $n - k$ Prüfzeichen hinzugefügt.

Charakterisierung durch Zahlentripel: $[n, k, d]$

d: Distanz, die angibt wie sehr sich je zwei Codeworte voneinander unterscheiden

Beispiel: $\mathcal{C} = \{(0, 0, 0), (1, 1, 1)\}$

Binärer Code mit zwei Codeworten.
Distanzfunktion: Hammingdistanz
Die Hammingdistanz gibt die Anzahl der Stellen an, an denen sich zwei Codeworte mindestens unterscheiden.

$\Rightarrow$ Code ist ein binärer $[3, 1, 3]$-Code.

Kanal mit Codierung:

$\mathbf{m}$	$\mathbf{c}$	$\mathbf{r}$	$\hat{\mathbf{c}}$	$\hat{\mathbf{m}}$
0	000	010	000	0

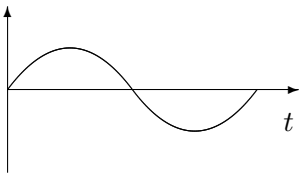
Aufgabe des Decodierers ist, das Codewort $\mathbf{c}$ zu finden, das dem empfangenen Vektor $\mathbf{r}$ am "nächsten"ist.

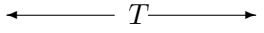
Im Beispiel ist die Hammingdistanz zwischen $\mathbf{r}$ und $(0, 0, 0)$ gleich 1 und zwischen $\mathbf{r}$ und $(1, 1, 1)$ gleich 2, sodass sich der Decodierer für $(0, 0, 0)$ also für das gesendete Bit 0 entscheidet.

Beispiele guter binärer Codes mit kurzer Länge: $[7, 4, 3]$, $[15, 11, 3]$, $[16, 8, 5]$, $[23, 12, 7]$

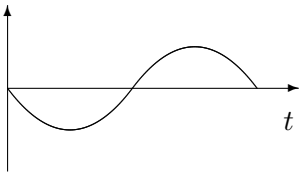
Zur Übertragung von 0101 . . .

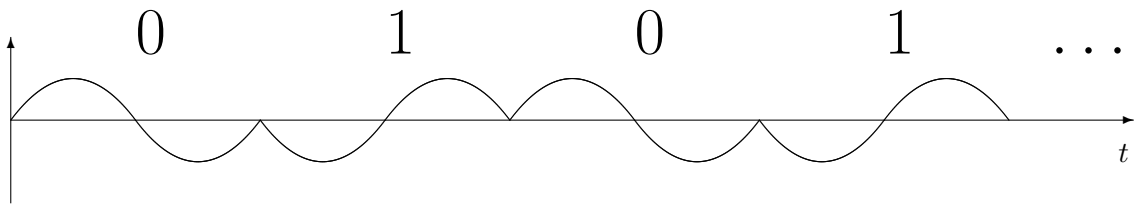
0: sende $f(t) = \sin \omega t$



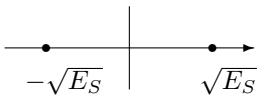


1: sende $f(t) = -\sin \omega t$





entsprechende Signalkonstellation:



$E_S = \int_0^T f(t)^2 dt$

Fehlerrate bei der Übertragung hängt ab vom Abstand der Signalpunkte.

Um Datenrate zu erhöhen:

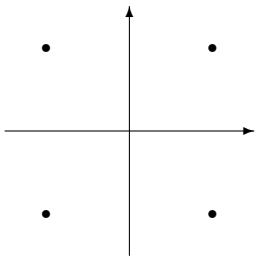
i. $f_i(t) = a_i \sin \omega t$

Signalkonstellation: 

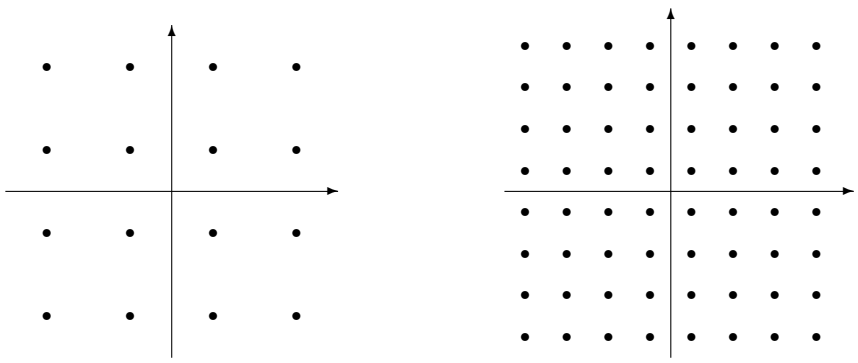
Bei gleicher Sendeleistung: höhere Fehlerwahrscheinlichkeit.

ii. eine Dimension höher gehen

00:	sende	$\sin \omega t + \cos \omega t$
01:	sende	$\sin \omega t - \cos \omega t$
10:	sende	$-\sin \omega t + \cos \omega t$
11:	sende	$-\sin \omega t - \cos \omega t$

Signalkonstellation:  4-QAM

16-QAM 64-QAM



16-QAM: jeder Signalpunkt überträgt 4 Bit

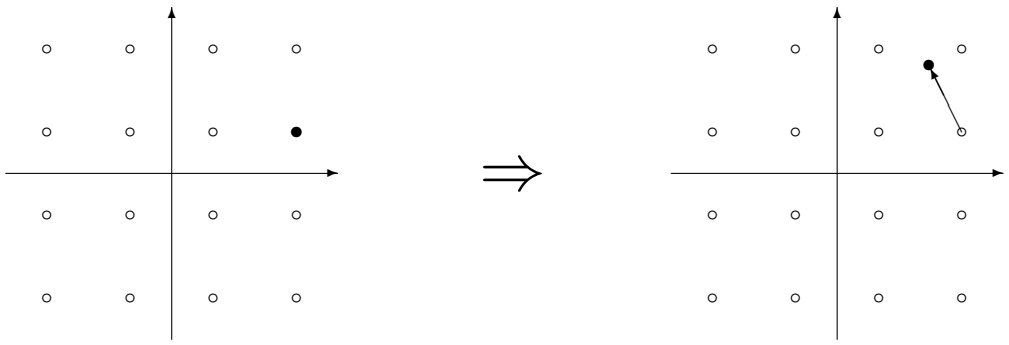
64-QAM: jeder Signalpunkt überträgt 6 Bit

Rückgewinnung der Information:

$$f(t) = m_1 \cdot \sin \omega t + m_2 \cdot \cos \omega t$$

$$f(t) \rightarrow \begin{cases} \boxed{\int f(t) \sin \omega t \, dt} \longrightarrow m_1 \\ \boxed{\int f(t) \cos \omega t \, dt} \longrightarrow m_2 \end{cases}$$

16-QAM



In Beispiel: Der gesendete Signalpunkt wird zu einem Nachbarsignalpunkt verfälscht.

Blockcodes mit der Hammingdistanz sind zur Codierung von QAM-Signalen nicht geeignet.

Geeignet ist die Euklidische Distanz, die algebraisch schlecht handhabbar ist.

Gut geeignet: Mannheim Distanz

Modulo-Rechnung:
Allseits bekannt von Uhrzeit und Kalender

Wenn man modulo von Primzahlen p rechnet erhält man sogenannte endliche Körper.

Endliche Körper sind besonders beliebt in der Codierung, da man damit besonders effiziente Codes konstruieren kann, die einfach codiert und decodiert werden können.

Endliche Körper mit p Elementen werden oft mit $GF(p)$ bezeichnet.

einfachstes Beispiel: $p = 2$

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

weiteres Beispiel: $p = 3$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$GF(3) = \{0, 1, 2\}$ mit Addition und Multiplikation modulo 3 ist ein endlicher Körper.

Andere Darstellungsform: $GF(3) = \{-1, 0, 1\}$

$+$	0	1	-1
0	0	1	-1
1	1	-1	0
2	-1	0	1

$\cdot$	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

Für Codierung von QAM-Signalen ist eine zweidimensionale Darstellung von endlichen Körpern besonders interessant.

Fermats berühmter Zwei-Quadrate-Satz:

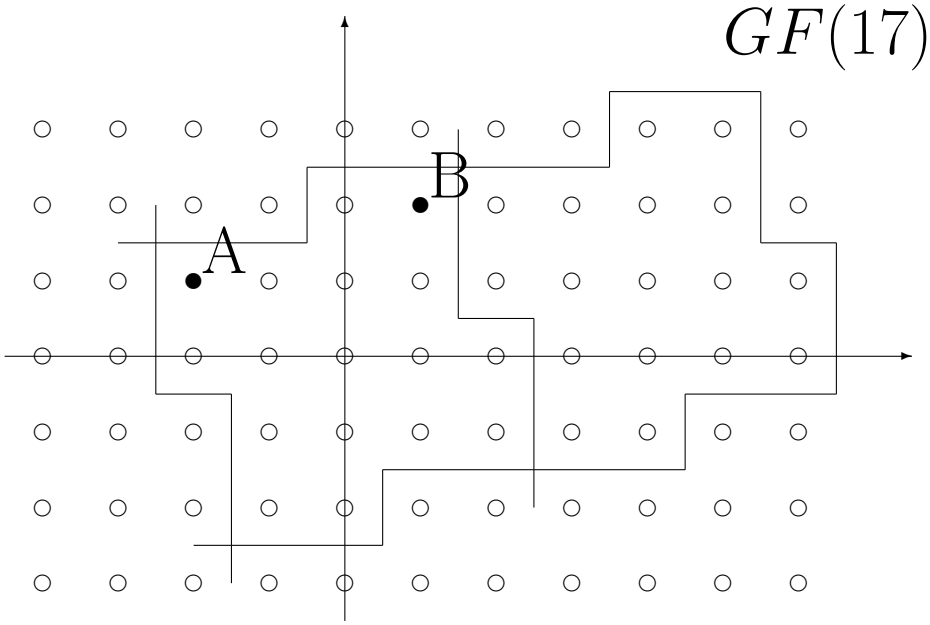
Jede Primzahl der Form $p \equiv 1 \bmod 4$ lässt sich im wesentlichen eindeutig als Summe von zwei Quadraten darstellen.

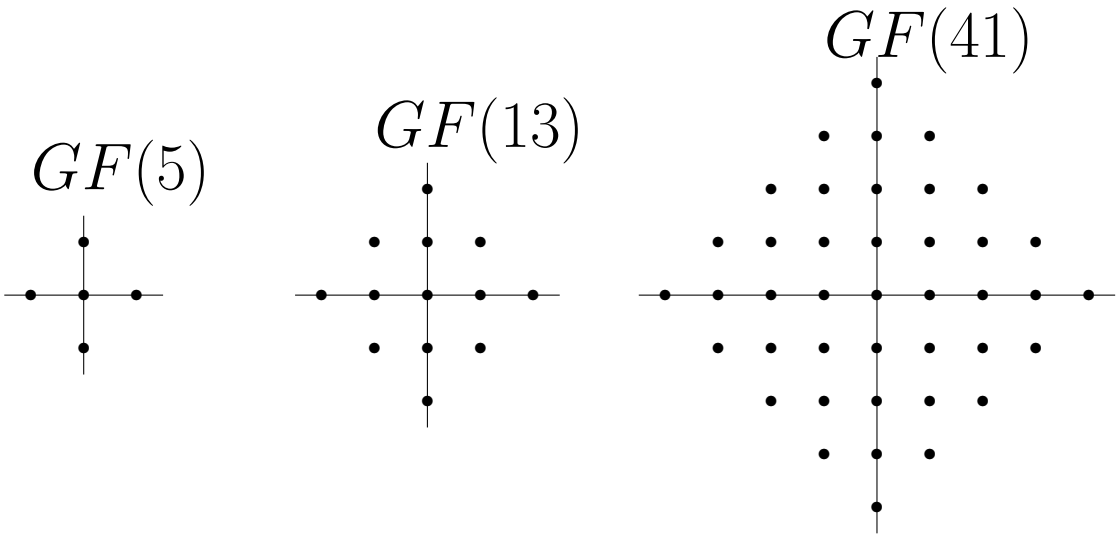
$$p = a^2 + b^2$$

Beispiele:

$$\begin{aligned} 5 &= 2^2 + 1^2 \\ 13 &= 3^2 + 2^2 \\ 17 &= 4^2 + 1^2 \\ 29 &= 5^2 + 2^2 \\ 37 &= 6^2 + 1^2 \\ 41 &= 5^2 + 4^2 \end{aligned}$$

Zweidimensionale Darstellung von $GF(p)$ und Mannheim Distanz





Die Mannheim Distanz

Sinn: algebraischer Zugang für Blockcodes über QAM-Signalkonstellationen.

$\Rightarrow$ bessere, effizientere Blockcodes

Mannheim Distanz = Manhattan Distanz modulo eines zweidimensionalen Gitters

In Beispiel auf voriger Seite:

Manhattan Distanz von A und B:

$d_{\text{Manhattan}}(A, B) = 3 + 1 = 4$

Mannheim Distanz von A und B:

$d_{\text{Mannheim}}(A, B) = 1$

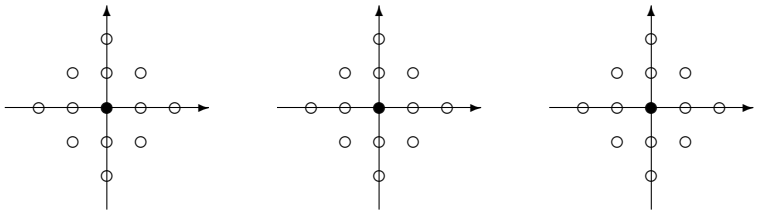
Distanzberechnung modulo $\text{mod} 4 + \imath$.

Block Codes für die Mannheim Distanz

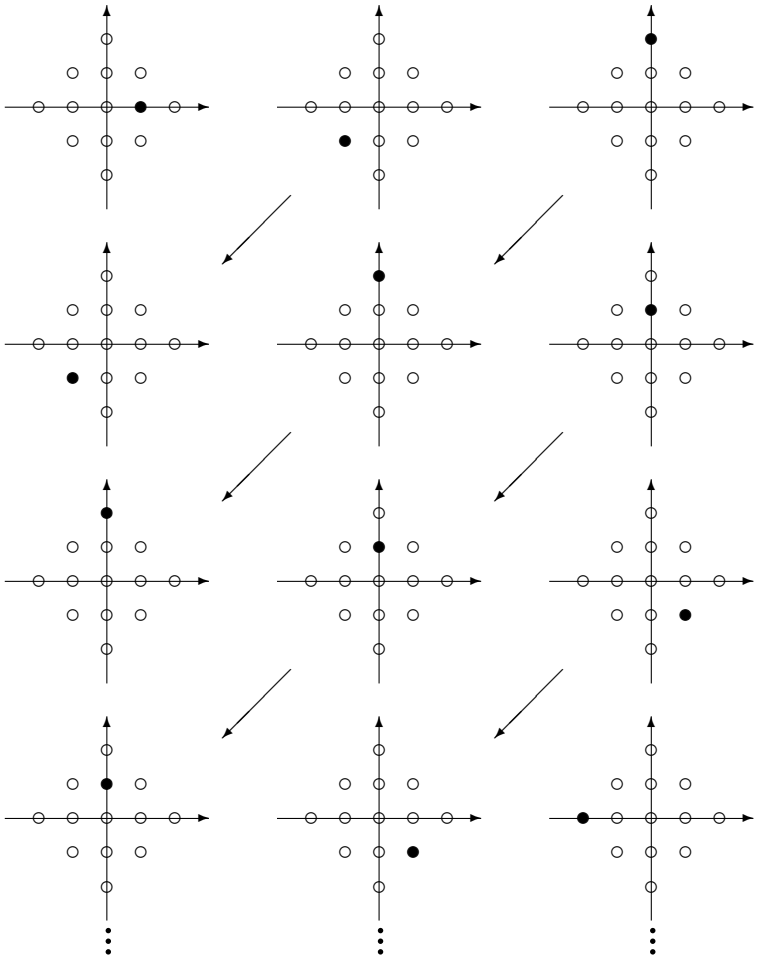
p	$[n, k, d_M]$
13	$[3, 1, 5]$
	$[3, 2, 3]$
17	$[4, 1, 8]$
	$[4, 2, 4]$
	$[4, 3, 3]$
29	$[7, 1, 19]$
	$[7, 2, 7]$
	$[7, 3, 7]$
	$[7, 4, 6]$
	$[7, 5, 4]$
	$[7, 6, 3]$
37	$[9, 1, 24]$
	$[9, 2, 17]$
	$[9, 3, 15]$
	$[9, 4, 6]$
	$[9, 5, 6]$
	$[9, 6, 6]$
	$[9, 7, 3]$
	$[9, 8, 3]$
41	$[10, 1, 30]$
	$[10, 2, 17]$
	$[10, 3, 17]$
	$[10, 4, 14]$
	$[10, 5, 11]$
	$[10, 6, 8]$
	$[10, 7, 6]$
	$[10, 8, 4]$
	$[10, 9, 3]$

Alle Codes sind *izyklische Codes*.

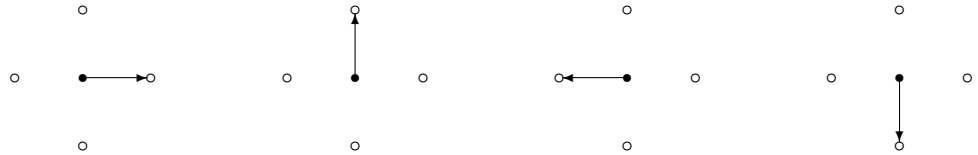
Beispiel: izyklischer $[3, 1, 5]$ Code über $GF(13)$
Codeworte sind das Nullwort:



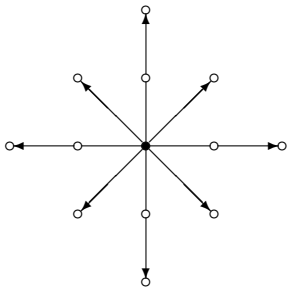
sowie die 12 izyklischen Verschiebungen von:



Mit dem $[3, 1, 5]$ Code können zwei Einzelfehler der Gestalt



oder ein Doppelfehler der Gestalt



korrigiert werden.

(Das heißt für $GF(13)$ ein beliebiger Doppelfehler).

Literatur

[1] R.E.Blahut, 'Digital Transmission of Information', Addison-Wesley, 1990.

[2] C.F.Gauss, Untersuchungen über Höhere Arithmetik", (Deutsche Übersetzung der lateinischen Disquisitiones Arithmeticae H.Maser1889), Chelsea Publishing Company, second reprint 1981, New York.

[3] C.F.Gauss, 'Theorie der biquadratischen Reste', Erste Abhandlung", Commentationes soc. reg. Gotting.recentiores. Vol.VI. Gottengae 1828, (enthalten in [2]).

[4] C.G.Gauss, 'Theorie der biquadratischen Reste', Zweite Abhandlung", Commentationes soc. reg. Gotting.recentiores. Vol.VII. Gottengae 1832, (enthalten in [2]).

[5] G.H.Hardy, E.M.Wright, 'An introduction to the theory of numbers', fifth edition, Oxford 1979.

[6] K.Huber, 'Codes over Gaussian Integers', IEEE Transactions on Information Theory, Vol.40, No.1, January 1994, pp.207-216.

[7] K.Huber, Codes over Eisenstein-Jacobi Integers", Finite Fields: Theory, Applications and Algorithms, (Las Vegas 1993), Contemporary Math. Vol.168, American Math. Society, Providence, RI, 1994, pp.165-179.

[8] K.Huber, Problem 10497, American Mathematical Monthly, January 1996, p.75.
Solution: American Mathematical Monthly, February 1998, p.185.

[9] K.Huber, 'The MacWilliams Theorem for Two-Dimensional Modulo Metrics', AAECC, Vol.8 No.1, pp. 41-48, 1997.

[10] K.Huber, 'Codes over Tori', IEEE Trans. on Inf. Theory, Vol.43, No.2, March 1997, pp.740-744.

[11] K.Huber: 'Efficient Utilisation of Multilevel Signal Constellations', International Symposium on Information Theory, MIT, August 16-21,1998.

[12] K.Huber, "Decoding of Icyclic Codes", ISITA conference, Parma, October 10-13, 2004, pp.1337-1340.

[13] V.Pless, W.C.Huffman, R.A.Brualdi, 'Handbook of Coding Theory I/II', North-Holland Publishing Co, 1998

[14] R.N.Roth, 'Introduction to Coding Theory', Cambridge University Press, 2006.

[15] C.E.Shannon , 'A Mathematical Theory of Communication', Bell Syst. Tech. J. 27 (1948) : 379-423 (Teil I), 623-656 (Teil II).