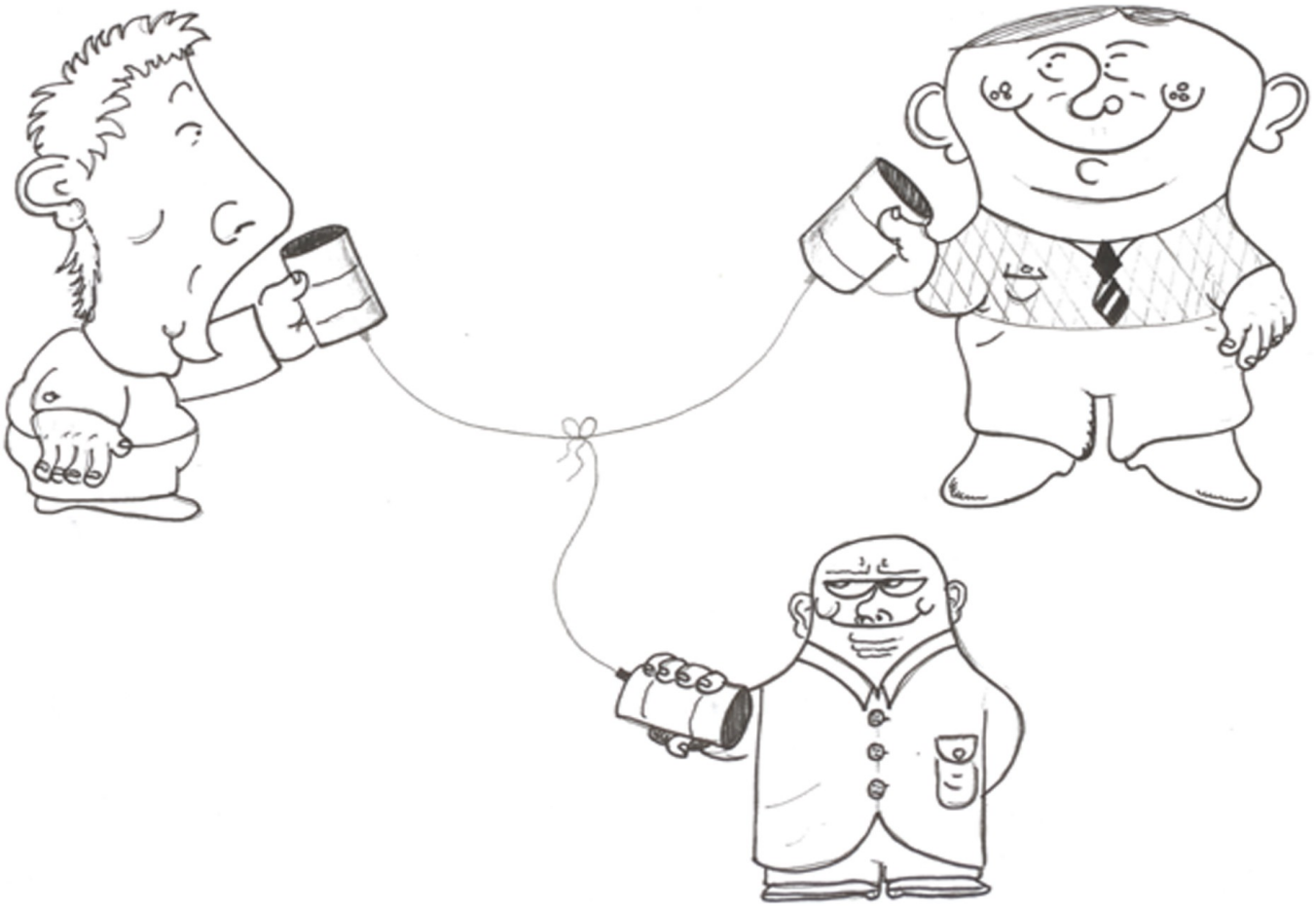
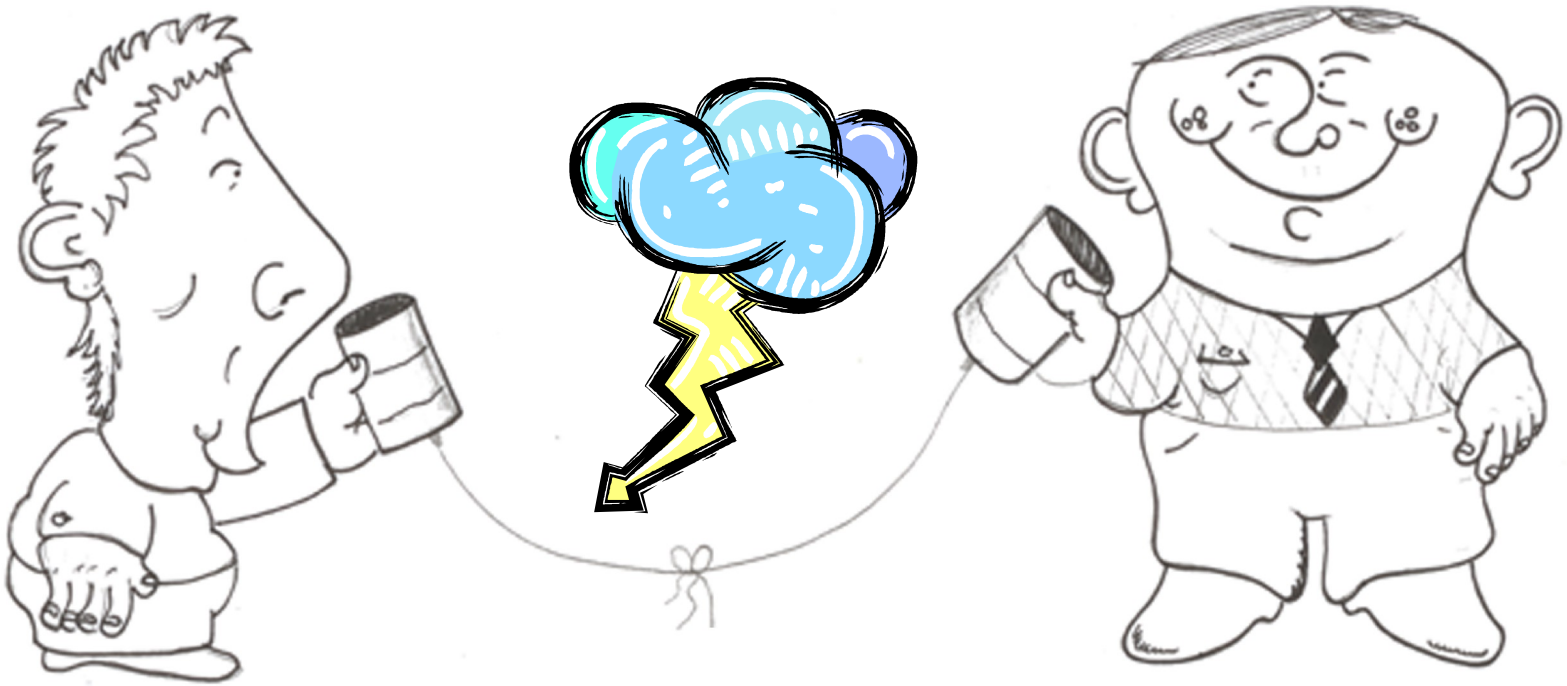
Codierungstheorie

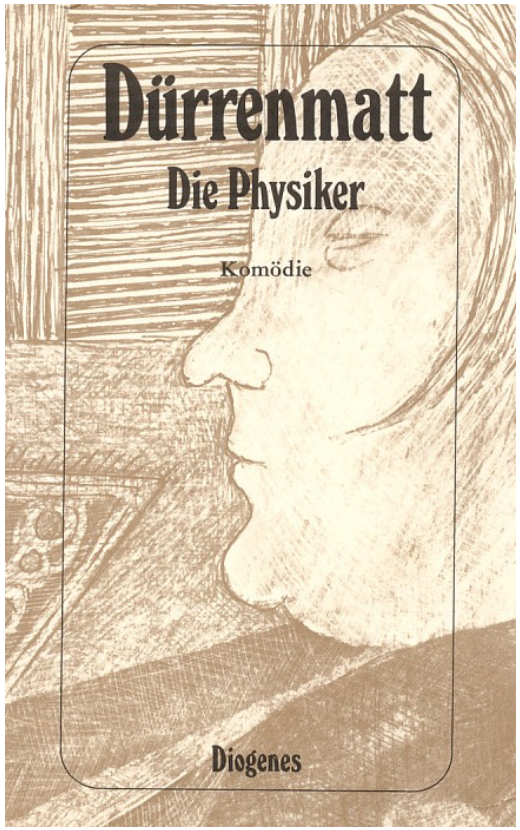
Kryptographie



Codierungstheorie



„Die Physiker“ von F. Dürrenmatt



ISBN

(Internationale

Standard Buchnummer)

$3 - 257 - 20837 - 5$

$$3\cdot 10 + 2\cdot 9 + 5\cdot 8 + 7\cdot 7 + 2\cdot 6 + 0\cdot 5 + 8\cdot 4 + 3\cdot 3 + 7\cdot 2 + p\cdot 1 = 0 \bmod 11$$

$$204 + p = 0 \bmod 11$$

$$209 = 0 \bmod 11$$

ISBN

$$10a_{10} + 9a_9 + 8a_8 + 7a_7 + 6a_6 + 5a_5 + 4a_4 + 3a_3 + 2a_2 + a_1 = 0 \bmod 11$$

alternativ:

$$a_{10} + 2a_9 + 3a_8 + 4a_7 + 5a_6 + 6a_5 + 7a_4 + 8a_3 + 9a_2 + 10a_1 = 0 \bmod 11$$

und somit

$$a_1 = a_{10} + 2a_9 + 3a_8 + 4a_7 + 5a_6 + 6a_5 + 7a_4 + 8a_3 + 9a_2 \bmod 11$$

Fehlererkennung und -korrektur (erste Schritte)

Die ISBN 0-387-96704-3 ist eine ungültige ISBN, da

$10 \cdot 0+9 \cdot 3+8 \cdot 8+7 \cdot 7+6 \cdot 9+5 \cdot 6+4 \cdot 7+3 \cdot 0+2 \cdot 4+3 = 263 = =$

$10 \neq 0 \mod 11$

Bei der ISBN 0-387-94704-? berechnet sich die Prüfziffer zu:

$a_1 = 0+2 \cdot 3+3 \cdot 8+4 \cdot 7+5 \cdot 9+6 \cdot 4+7 \cdot 7+8 \cdot 0+9 \cdot 4 = 212 = = 3$

$\mod 11$

Fehlererkennung und -korrektur (erste Schritte)

Bei der ISBN 0-397-6?704-3 ist eine Ziffer an einer bestimmten Stelle unbekannt:

$10\cdot 0+9\cdot 3+8\cdot 9+7\cdot 7+6\cdot 6+5\cdot x+4\cdot 7+3\cdot 0+2\cdot 4+3=5\cdot x+223$

$= 5\cdot x + 3 = 0 \mod 11 \quad | + 8$

$5\cdot x + 11 = 8 \mod 11 \quad | \cdot 9$

$45\cdot x = 72 \mod 11 \Rightarrow x = 6 \mod 11$

Jedoch gibt es bei einer fehlerhaften ISBN (etwa: 0-387-96704-3) keine Möglichkeit zur Korrektur, außer man kennt die Stelle des Fehlers.

Welche Fehler werden erkannt?

Einzelfehler: 3-287-20837-5 statt 3-257-20837-5

Nachbarschaftsvertauschung:

3-275-20837-5 statt 3-257-20837-5

Allgemeine Drehfehler:

3-287-20537-5 statt 3-257-20837-5

Begründung?

Einzelfehler

$a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$ korrekte ISBN

$a'_{10}\ a'_9\ a'_8\ a'_7\ a'_6\ a'_5\ a'_4\ a'_3\ a'_2\ a'_1$ ISBN mit Fehler an der i-ten Stelle, auch als korrekt angenommen

$$10a_{10} + 9a_9 + 8a_8 + 7a_7 + 6a_6 + 5a_5 + 4a_4 + 3a_3 + 2a_2 + a_1 = 0 \bmod 11$$

$$10a'_{10} + 9a'_9 + 8a'_8 + 7a'_7 + 6a'_6 + 5a'_5 + 4a'_4 + 3a'_3 + 2a'_2 + a'_1 = 0 \bmod 11$$

Subtrakion liefert:

$$i\,a_i - i\,a'_i = i\,(a_i - a'_i) = 0 \bmod 11$$

$i \in \{1; 2; \ldots ; 9\}$ und $a_i - a'_i \in \{-10; -9; \ldots ; -1; 1; 2; \ldots ; 9; 10\}$, also

$$a_i - a'_i = 0 \bmod 11 \quad \Rightarrow \quad a_i = a'_i$$

Allgemeiner Drehfehler

$a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$ korrekte ISBN

$a'_{10}\ a'_9\ a'_8\ a'_7\ a'_6\ a'_5\ a'_4\ a'_3\ a'_2\ a'_1$ ISBN mit Vertauschung an der i-ten und j-ten Stelle, auch als korrekt angenommen

$10a_{10} + 9a_9 + 8a_8 + 7a_7 + 6a_6 + 5a_5 + 4a_4 + 3a_3 + 2a_2 + a_1 = 0 \bmod 11$

$10a'_{10} + 9a'_9 + 8a'_8 + 7a'_7 + 6a'_6 + 5a'_5 + 4a'_4 + 3a'_3 + 2a'_2 + a'_1 = 0 \bmod 11$

Subtrakion liefert:

$i\,a_i + j\,a_j - i\,a'_i - j\,a'_j = i\,a_i + j\,a_j - i\,a_j - j\,a_i = i\,(a_i - a_j) - j\,(a_i - a_j) =$

$= (i - j)\,(a_i - a_j) = 0 \bmod 11$

$i - j \in \{-9; -8; \ldots; -1; 1; 2; \ldots; 9\}$ und $a_i - a_j \in \{-10; \ldots; -1; 1; \ldots; 10\}$,

also $a_i - a_j = 0 \bmod 11 \Rightarrow a_i = a_j$

Die Europäische Artikelnummer EAN

9780387947044

$$a_{13}\ a_{12}\ a_{11}\ a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$$

Mit der Prüfgleichung

$$a_{13} + 3 \cdot a_{12} + a_{11} + 3 \cdot a_{10} + a_9 + 3 \cdot a_8 + a_7 + 3 \cdot a_6 + a_5 + 3 \cdot a_4 + a_3 + 3 \cdot a_2 + a_1 = 0 \bmod 10$$

Die Europäische Artikelnummer EAN

9780387947044

$$a_{13}\ a_{12}\ a_{11}\ a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$$

Mit der Prüfgleichung

$$9 + 3\cdot 7 + 8 + 3\cdot 0 + 3 + 3\cdot 8 + 7 + 3\cdot 9 + 4 + 3\cdot 7 + 0 + 3\cdot 4 + 4 =$$

$$= 140 = 0 \bmod 10$$

Aufgaben zur EAN

1) Ist die EAN 9381377142703 gültig?
2) Bestimme die Prüfziffer p in 735294412935p.
3) Korrigiere den Fehler x in 73529x4149354.
4) Welche Fehler werden vom EAN-Verfahren erkannt? Beweis?
5) Was ändert sich, wenn man im EAN-Verfahren die 3 durch eine 2 ersetzt, welche Fehler werden nun von diesemVerfahren erkannt? Beweis?
6) Die 3 durch 5, durch 7 .... ersetzen?!?

Kontonummernsysteme

Es gibt verschiedene Prüfgleichungen.

Einige Verfahren sind dem EAN sehr ähnlich, andere benutzen die Quersumme (hier mit Q bezeichnet, also Q(12)=3).

Kontonummernsysteme

1. Weg: 19645524

$$a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$$

Mit der Prüfgleichung

$$2\cdot a_8+a_7+2\cdot a_6+a_5+2\cdot a_4+a_3+2\cdot a_2+a_1=0 \bmod 10$$

$$2\cdot 1+9+2\cdot 6+4+2\cdot 5+5+2\cdot 2+4 =50=0 \bmod 10$$

Kontonummernsysteme

2. Weg: 19645522

$$a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$$

Mit der Prüfgleichung

$$Q(2\cdot a_8)+a_7+Q(2\cdot a_6)+a_5+Q(2\cdot a_4)+a_3+$$

$$Q(2\cdot a_2)+a_1=0 \bmod 10$$

$$Q(2)+9+Q(12)+4+Q(10)+5+ Q(4)+2=0 \bmod 10$$

$$2 + 9 + 3 + 4 + 1 + 5 + 4 + 2 = 30 = 0 \bmod 10$$

Kontonummernsysteme

Man kann Q(2·x) auch als Permutation schreiben:

$$Q = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 0 & 2 & 4 & 6 & 8 & 1 & 3 & 5 & 7 & 9 \end{pmatrix}$$

Die alten DM-Scheine - Diedergruppe

Es wird die Symmetriegruppe D_5 des Fünfecks mit ebenfalls 10 Elementen verwendet.

Wie rechnet man in D_5?

Man benötigt auch Permutationen!

Die alten DM-Scheine - Diedergruppe

Es wird die Symmetriegruppe D_5 des Fünfecks mit ebenfalls 10 Elementen verwendet.

Wie rechnet man in D_5? Mit einem Fünfeck!

Man benötigt auch Permutationen! Die mischen die Zahlen nur kräftig durch.

Berechnung

DG6244129Y1

12624412981

allgemein

$$a_{11}\ a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$$

mit der Prüfgleichung

$$T(a_{11})*T^2(a_{10})*T^3(a_9)*T^4(a_8)*T^5(a_7)*T^6(a_6)*T^7(a_5)*$$
$$T^8(a_4)*T^9(a_3)*T^{10}(a_2)*\ a_1 = 0$$

$$T(1)*T^2(2)*T^3(6)*T^4(2)*T^5(4)*T^6(4)*T^7(1)$$
$$*T^8(2)*T^9(9)*T^{10}(8)*\ 1 = 0$$

Berechnung

DG6244129Y1

5 * 0 * 3 * 5 * 5* 8 * 0 * 2 * 4 * 4 * 1 = 0

5 * 8 * 5* 8 * 0 * 2 * 4 * 4 * 1 = 0

2 * 2* 2 *3 * 1 = 0

4 * 0 * 1 = 0

4 * 1 = 0

Aufgaben

1) Berechne $a^{2}ba^{2}b^{5}a^{12}bbba^{3}a^{4}$ mit dem Fünfeck!
2) Prüfe die Tabelle.
3) Handelt es sich bei DG4266124Y3 um eine korrekte Nummer auf einem DM-Schein?
4) Bereche das fehlende Zeichen: DG1234567?1. Es handelt sich dabei um einen Buchstaben!
5) Warum gibt es dieses Verfahren beim Euro nicht mehr?

Vergleich der Verfahren

	Verwechslung einer Ziffer	Drehfehler (Nachbarziffer)	Allgemeiner Drehfehler
ISBN	immer	immer	immer
EKONS (1.Weg)	in Sonder-fällen nicht	immer	selten
EKONS (2.Weg)	immer	in Sonder-fällen nicht	selten
EAN	immer	in Sonder-fällen nicht	selten
Geldschein	immer	immer	in Sonder-fällen nicht

Andere Interpretation, etwa der ISBN:

Aus allen möglichen Wörtern

$$a_{10}\ a_9\ a_8\ a_7\ a_6\ a_5\ a_4\ a_3\ a_2\ a_1$$

der Länge 10 mit 11 Buchstaben {0,1,2,3,4,5,6,7,8,9,X} werden die „richtigen“ ausgewählt.

Nur a_1 darf mit X belegt werden.

Es muss die Prüfgleichung

$$10\cdot a_{10} +9\cdot a_9 +8\cdot a_8 +7\cdot a_7 +6\cdot a_6 +5\cdot a_5 +4\cdot a_4 +3\cdot a_3 +2\cdot a_2 +1\cdot a_1 = 0 \bmod 11$$

gelten.

Andere Interpretation:

Der Code C (der „richtigen Codewörter“) ist also eine Teilmenge aller Wörter der Länge 10.

$$C \subset \{0,1,2,3,4,5,6,7,8,9,X\}^{10}$$

Vertiefung dieser Interpretation

Man benötigt ein Alphabet A der Länge r, z.B. {A,B,C,D,… Z} (r=26) oder {0,1,2,3,…9} (r=10) oder Z/2Z (r=2) oder….

Ein Code C ist eine Teilmenge von A^n.

Man nennt n die Länge der Codewörter.

Die Anzahl der Codewörter ist M mit $M = |C|$.

Der Hammingabstand zweier Codewörter, ist die Anzahl der Fehlstände:

d(rot, tot) =1; d(12345, 54321) =4; d(01,01)=0

Ein r-ärer (n,M,d)-Code

Der Minimalabstand eines Codes C, ist das Minimum aller (versch.) Abstände.

C = {0000, 0011, 1100, 1111}

d = 2

also ein (4,4,2)-Code

C = {0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111}

d = 2

also ein (4,8,2)-Code

Es werden nun Codes mit vorgegebenen Parametern r, n und d gesucht. Dabei soll M möglichst groß sein.

Aufgaben zum (n,M,d)-Code

1)C={00011, 00101, 11101,11000}

r=2; n=?; M=?; d=?

2)C={00000, 11111}

r=3; n=?; M=?; d=?

3)C={00, 01, 10, 11}

r=2; n=?; M=?; d=?

4) Gib jeweils einen binären (n,M,d)-Code an mit

(8,2,8); (8,3,8); (3,9,1);

(4,8,2); (5;3;4).

Fehlerkorrektur mit dem Hamming-Abstand

C= {0000,0011,1000,1100}

empfangen: x = 0111

d(0000,0111) = 3

d(0011,0111) = 1

d(1000,0111) = 4

d(1100,0111) = 3

Decodierung : c = 0011

Aufgabe zur Decodierung

1) C = {0000, 1100, 1010, 1001, 0110, 0101, 0011, 1111}

Empfangen: 1101

2) C = $Rep_3(4)$ = {0000, 1111, 2222}

Empfangen: 2111

Empfangen: 2121

Die Suche nach $A_r(n,d)$

Die größte Codelängen M bezeichnet man mit

$A_r(n,d)$

Beispielsweise:

$A_5(7,7) = 5$

allgemeiner $A_r(n,n) = r$

$A_r(n,1) = r^n$

$A_2(5,3) = 4$

$C = \{00000, 11100, 00111, 11011\}$

Ein (32,64,16)-Code wurde 1972 von Mariner 9 benutzt um Bilder vom Mars zu senden

Aufgabe zu $A_r(n,d)$

Begründe:

1) $A_2(6,5) = 2$
2) $A_2(7,5) = 2$
3) $A_2(8,5) = 4$
4) $A_r(n,n) = r$

Schranken für $A_r(n,d)$

- Singleton-Schranke:

$$A_r(n,d) \leq r^{n-d+1}$$

- Plotkin-Schranke:

$$A_2(n,d) \leq 2\left[\frac{d}{2d-n}\right]$$

- Kugelpackungs-Schranken:

$$\frac{r^n}{V_r^n(d-1)} \leq A_r(n,d) \leq \frac{r^n}{V_r^n\left(\left[\frac{d-1}{2}\right]\right)}$$

mit Kugelvolumen $V_r^n(\rho) = \sum_{k=0}^{\rho} \binom{n}{k} (r-1)^k$

Offene Fragen

$A_2(n,d)=$

n	d=3	d=5	d=7
7	16	2	2
9	40	6	2
11	144-158	24	2
15	2048	256	32
16	2560-3276	256-340	36-37

Exakte Sequenz

Für einen linearen r-ären (n,r^k,d)-Code hat man die Z/rZ-lineare Einbettung $(Z/rZ)^k \rightarrow (Z/rZ)^n$ und erhält man die exakte Sequenz

$$0 \rightarrow (Z/rZ)^k \xrightarrow{C^t} (Z/rZ)^n \xrightarrow{H} (Z/rZ)^{n-k} \rightarrow 0$$

Man nennt C die Erzeugermatrix und H die Prüfmatrix des Codes.

(so schnell sind viele Lehrbücher)

Zwei „Arten“ von Matrizen

Eine Prüfmatrix ist die Kurzschrift eines Gleichungssystems:

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Der Code ist dessen Lösungsmenge:

C= {0000000, 1101001, 0101010, 1001100, 1100110, 0100101, 1000011, 0001111, 1110000, 0011001, 1010101, 0110011, 0010110, 1011010, 0110011, 1111111}

Zwei „Arten“ von Matrizen

Aus der Erzeugermatrix entsteht der Code durch Addition aller möglichen Kombinationen von Vielfachen der Zeilen:

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

C= {0000000, 1101001, 0101010, 1001100,
1100110, 0100101, 1000011, 0001111, 1110000,
0011001, 1010101, 0110011, 0010110, 1011010,
0110011, 1111111}

Aufgaben zu den Matrizen

1) Welcher Code ist durch diese Prüfmatrix gegeben?

$$H = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

2) Welcher Code ist durch diese Erzeugermatrix gegeben?

$$C = \begin{pmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

3) Welcher Code ist durch diese Prüfmatrix gegeben?

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

4) Welcher Code ist durch diese Erzeugermatrix gegeben?

$$C = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Der Hamming-Code

Ein binärer Code mit mehreren Prüfstellen (z.B. der Hamming-(7,4)-Code oder auch H(3): ein (7,16,3)-Code):

p1	**p2**	**b3**	**p4**	**b5**	**b6**	**b7**

Im Folgenden wird die Entwicklung des Hamming-Codes vorgestellt, wie sie ein Schüler im W-Seminar vorgestellt hat.

Der Hamming-(7,4)-Code

- **Der bekannteste Hamming-Code**
- **Besteht aus insgesamt 7 Bits (n = 7)**

  4 Datenbits (k = 4)

  und 3 Prüfbits (r = 3)

Hamming-(7,4)-Code oder auch $H_2(3)$ definiert durch :

$$H := \begin{matrix} 1010101 \\ 0110011 \\ 0001111 \end{matrix}$$

Prüfmatrix

$$G := \begin{matrix} 1101001 \\ 0101010 \\ 1001100 \\ 1110000 \end{matrix}$$

Generatormatrix

Erstellen eines Codewortes

p1	p2	b3	p4	b5	b6	b7

ALICE erstellt ein Codewort :
Sie will eine Zahl Z = 10 zu BOB übertragen.
Dazu schreibt sie 10 im Dualsystem :

16	8	4	2	1
-	1	0	1	0

ALICE schreibt ihre Information 1010 als Datenbits im Hamming-Codewort :

p1	p2	1	p4	0	1	0

Um zu vermeiden, dass eine falsche Zahl übertragen wird, muss ALICE die Prüfdatenbits errechnen. So kann BOB später nachprüfen, ob sein erhaltenes Codewort stimmt.

ALICE benutzt die Kontroll-Matrix, um die Prüfbits p zu errechnen.

$$H := \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Erste Zeile : $c1 + c3 + c5 + c7 = 0$

Zweite Zeile : $c2 + c3 + c6 + c7 = 0$

Dritte Zeile: $c4 + c5 + c6 + c7 = 0$

$c1 = - c3 - c5 - c7 = c3 + c5 + c7$

$c2 = - c3 - c6 - c7 = c3 + c6 + c7$

$c4 = - c5 - c6 - c7 = c5 + c6 + c7$

p1	p2	1	p4	0	1	0

$c1 = c3 + c5 + c7 = 1 + 0 + 0 = 1$ Z / 2Z

$c2 = c3 + c6 + c7 = 1 + 1 + 0 = 0$ Z / 2Z

$c4 = c5 + c6 + c7 = 0 + 1 + 0 = 1$ Z / 2Z

$c1 = 1 = p1$

$c2 = 0 = p2$

$c4 = 1 = p4$

→ **ALICE** hat die Prüfbits erfolgreich errechnet

1	0	1	1	0	1	0

Der Code ist erstellt!

Fehlerkorrektur

ALICE versendet das Codewort an BOB.

1	0	1	1	0	1	0

Leider wird durch einen Übertragungsfehler ein Bit vertauscht.

1	0	1	1	1	1	0

BOB überprüft zur Sicherheit das Codewort. Dazu hat er 2 Möglichkeiten:

Methode 1 zur Fehlerkorrektur :

BOB überprüft die Prüfgleichungen.

1	0	1	1	1	1	0

c1 = c3 + c5 + c7 → 1 = 1 + 1 + 0 falsch

c2 = c3 + c6 + c7 → 0 = 1 + 1 + 0 wahr

c4 = c5 + c6 + c7 → 1 = 1 + 1 + 0 falsch

Gleichungen von c1 und c4 sind falsch =>

c5 ist falsch

1	0	1	1	X	1	0

Was muss BOB in c5 einsetzen, damit der Code stimmt ?

c1 = c3 + c5 + c7

$\Rightarrow$c5 = c1 – c3 – c7 = c1 + c3 + c7 = 1 + 1 + 0 = 0

1	0	1	1	0	1	0

Code erfolgreich korrigiert.

Methode 2 zur Fehlerkorrektur :

Skalarmultiplikation mit Prüfmatrix

1	0	1	0	0	1	0

Gedachter Rechenschritt:

$$1010010 \times \begin{bmatrix} 001 \\ 010 \\ 011 \\ 100 \\ 101 \\ 110 \\ 111 \end{bmatrix} = \begin{matrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ + & + & + \end{matrix} = 100\ (=4)$$

4.Stelle falsch

(anschließend mit Prüfgleichung c4 errechnen)

Decodierung

Nachdem BOB alle Fehler korrigiert hat, decodiert er.

1	**0**	**1**	**1**	**0**	**1**	**0**
--	--	1	--	0	1	0

BOB erhält eine von ALICE verschlüsselte Botschaft:
1010 (=10)

Ergänzungen zum Hamming-Code

Man verwendet geschickter die Prüfmatrix in folgender Form:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Man beachte, dass in den Spalten die Zahlen 1, 2, 3, 4, ... in binärer Schreibweise stehen.

tertiärer Hamming-Code $H_3(3)$

$$H_3(3)=\begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 2 & 2 & 2 \\ 1 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

Die Zahlen 1, 2, 3, 4, ... in tertiärer Schreibweise, jedoch nur mit führender Stelle 1.

Seminararbeit

All das und noch mehr findet sich in der Seminararbeit dieses Schülers:

Hamming-Code

Aufgaben zu Hamming-Codes

1) Stelle die Matrix zu $H_2(4)$ auf.
2) Stelle die Matrix zu $H_4(2)$ auf.
3) Decodiere 1100011 mit $H_2(3)$.

Weitere dezimale Codes

Wer noch nicht genug hat, kann die Seminararbeit eines anderen Schülers schauen:

Einige dezimale Codes

Englische Literatur

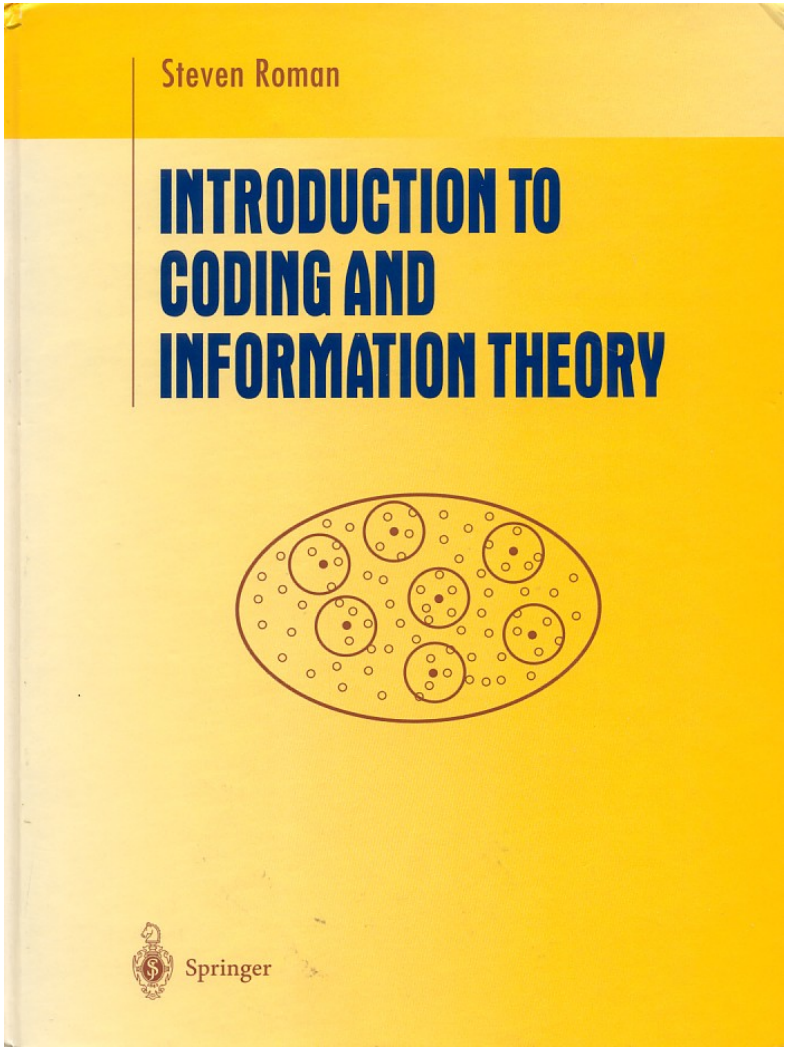
Steven Roman

Introduction

to Coding and

Information Theory

Springer (1997)



Weitere Literatur

- A. Beutelspacher, Luftschlösser und Hirngespinste, Vieweg (1986)
- F. Padberg, Elementare Zahlentheorie, Spektrum (1996)
- R.-H. Schulz, Codierungstheorie, Vieweg (1991)
- A. Bartholomé, J. Rung, H. Kern, Zahlentheorie für Einsteiger, Vieweg (2001)
- www.pruefziffernberechnung.de

Überblick zu den didaktischen Überlegungen

1) Kompetenzen
2) Projektunterricht
3) Schreiben im Mathematikunterricht: Dialogisches Lernen
4) Themenstudienarbeit
5) Allgemeinbildung und Bildungsstandards

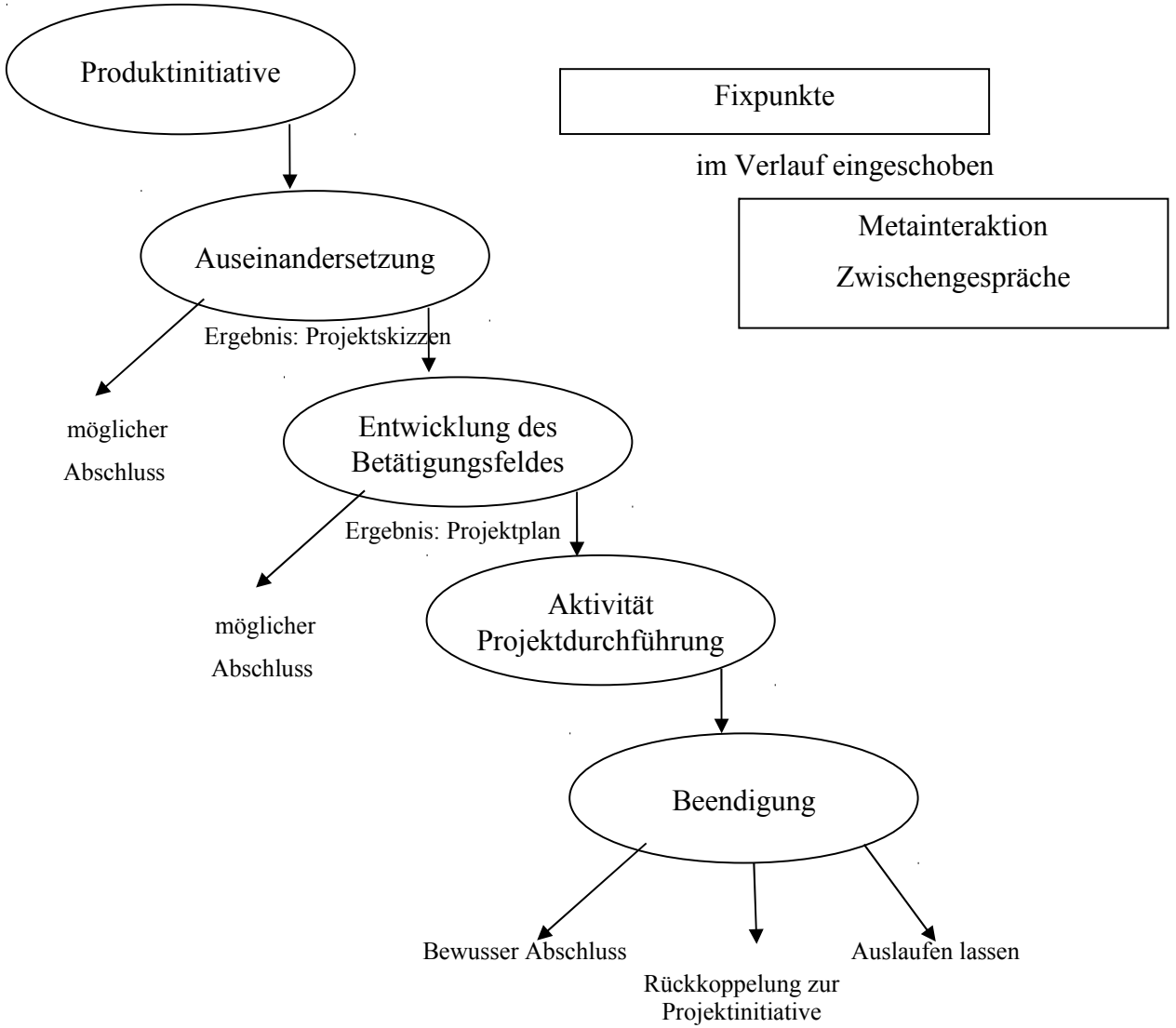
Kompetenzen (ISB München)

- Selbstkompetenz
- Sozialkompetenz
- Fachkompetenz
- Methodenkompetenz
  - geeignete didaktische Konzepte
  - schülergemäße Umsetzung der fachwissenschaftlichen Inhalte

Gudjons' Merkmalkatalog des Projektunterrichts

- Situationsbezug
- Orientierung an den Interessen der Beteiligten
- Gesellschaftliche Praxisrelevanz
- Zielgerichtete Projektplanung
- Selbstorganisation und Selbstverantwortung
- Einbeziehen vieler Sinne
- Soziales Lernen
- Produktorientierung
- Interdisziplinarität
- Grenzen des Projektunterrichts

Stufenmodell nach Frey



Projektunterricht

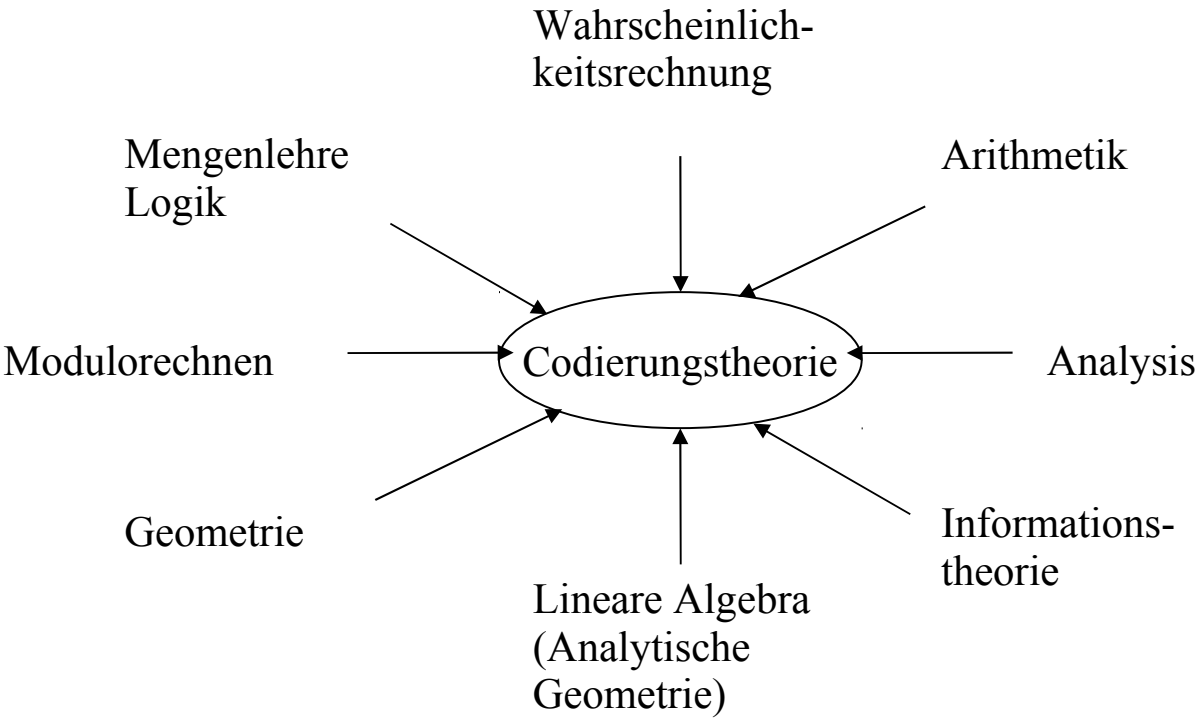
Besonders die auf unterrichtliche Praxis bezogenen Umsetzungsmöglichkeiten von Ludwig sind für die Gestaltung eines W-Seminars hilfreich.

Projekte im Mathematikunterricht können Veränderungen im schulischen und unterrichtlichen Bereich hervorrufen.

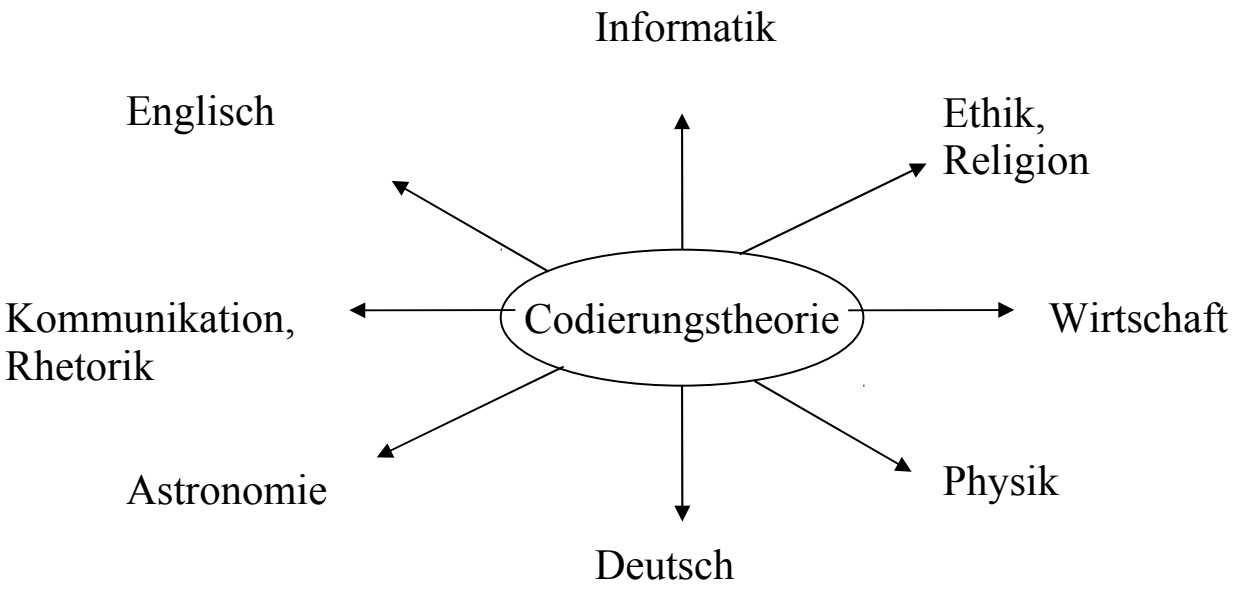
(Ludwig, 1998)

- Reflexion über das W-Seminar

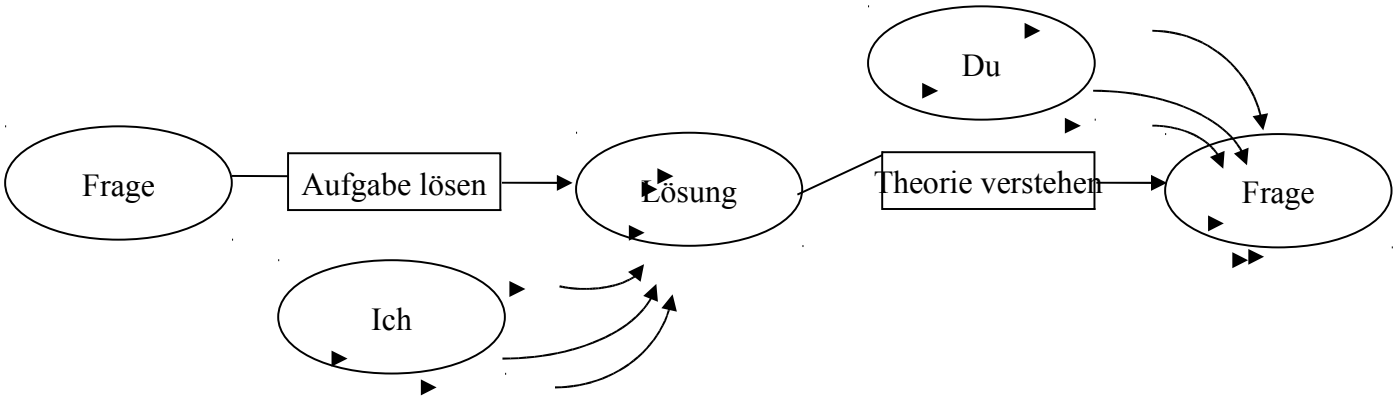
Magnetmodus nach Ludwig



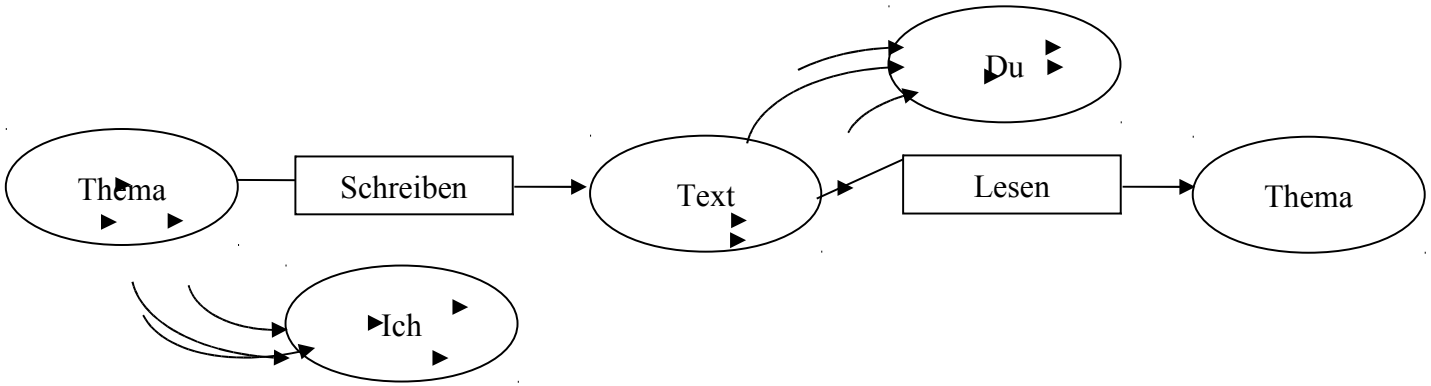
Sternmodus nach Ludwig



Dialogisches Lernen nach Gallin und Ruf (Ich-Du-Wir-Prinzip)

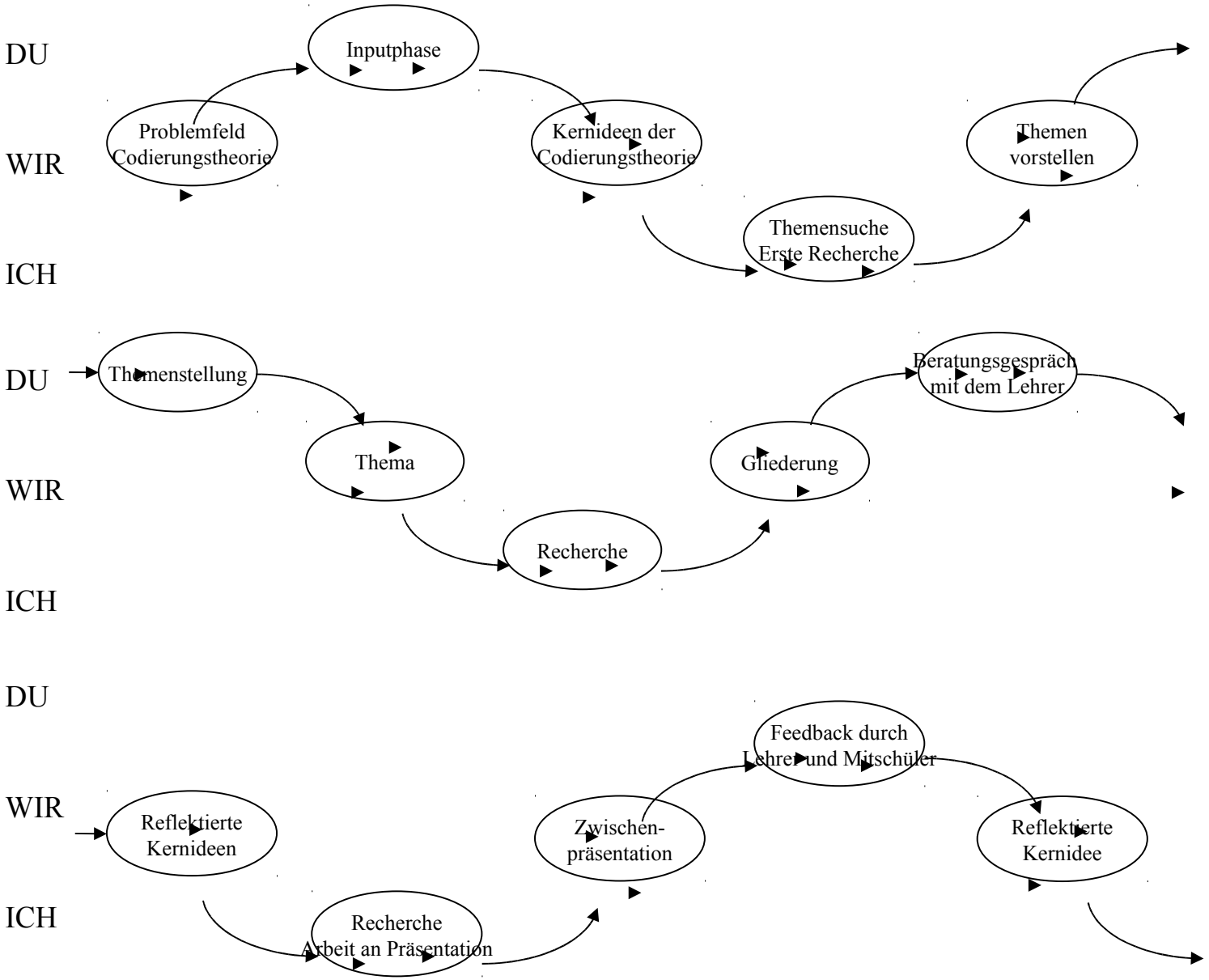


Dauerkonvergenz im Mathematikunterricht

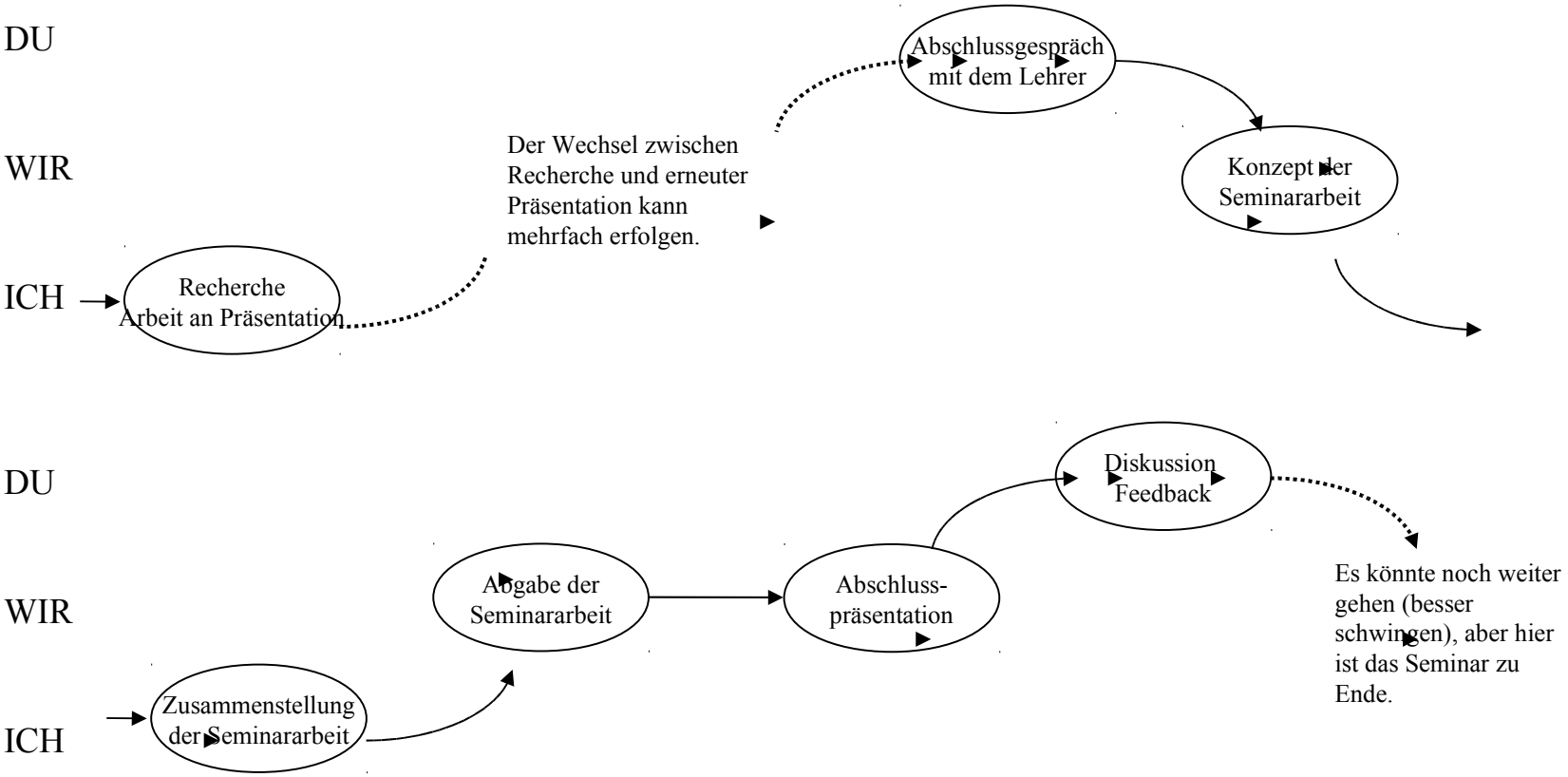


Dauerdivergenz im Deutschunterricht

Ich-Du-Wir-Prinzip am Beispiel des W-Seminars



Ich-Du-Wir-Prinzip am Beispiel des W-Seminars



Themenstudienarbeit nach Kuntze

Themenstudienarbeit

- Schüler setzen sich mit heterogenen Materialien auseinander
- Sie schreiben über ein mathematik-bezogenes Thema
- Verbindung zwischen der eigenen Persönlichkeit und Themen der Mathematik
- Dreiphasiger Aufbau: Ausgangspunkt, Arbeitsprozess, Ergebnis

Allgemeinbildender Mathematik-unterricht nach Heymann

- Lebensvorbereitung
- Stiftung kultureller Kohärenz
- Weltorientierung
- Denkenlernen und kritischer Vernunftgebrauch
- Entfaltung von Verantwortungsbereitschaft
- Einübung von Verständigung und Kooperation
- Ich-Stärke der Schüler

Bildungsstandards der KMK

mathematische Kompetenzen

- Mathematisch argumentieren
- Probleme mathematisch lösen
- Mathematisch modellieren
- Mathematische Darstellungen verwenden
- Mit Mathematik symbolisch, formal und technisch umgehen
- Mathematisch kommunizieren

Anforderungsbereiche

I. Reproduzieren

II. Zusammenhänge herstellen

III. Verallgemeinern und Reflektieren

Leitideen

- Zahl
- Messen
- Raum und Form
- Funktionaler Zusammenhang
- Daten und Zufall

W-Seminar mit Rahmenthema „Codierungstheorie“

- anspruchsvolles Thema
- guter Anwendungsbezug
- viele Möglichkeiten zur Programmierung
- Verwirklichung kompetenzorientierter und allgemeinbildender Aspekte

Zeitplanung im Schulversuch

- September 06 bis Dezember 06
  Inputphase (lehrerzentrierter Unterricht)
- Dezember 06
  1. Besprechung (Themenstellung)
- Januar 07
  2. Besprechung (erste Ergebnisse)
- Februar 07 bis April 07 (Seminarfahrt!)
  Referate (im G8 Zwischenpräsentation)
  Wertung als mündliche Note

Zeitplanung im Schulversuch

- Mai 07

  3. Besprechung (Feed-back für das Referat)

  4. Besprechung (Abschluss der Seminararbeit)
- Juni 07

  Abgabe der Seminararbeit

  Wertung als 4. Schulaufgabe

  (im G8 folgt noch eine Abschlusspräsentation)

analog im Schuljahr 2007/08

Mögliche Seminararbeiten

- Codierungstheorie bei Kontonummern verschiedener Institute
- Codierung bei den DM-Geldscheinen: Diedergruppe
- Huffman-Codierung
- Das Hauptproblem der Codierungstheorie - Berechnungen von $A_r(n,d)$
- Neue Codes aus alten Codes
- Die Singleton- und Plotkin-Schranken
- Hamming-Codes
- Reed-Muller-Codes
- Zyklische Codes

Benotung der Referate

- Eine Bewertungsmatrix kann helfen, dass die Notengebung für die Schüler nachvollziehbar wird.
- Meist schätzen sich die Schüler besser ein und es muss sorgfältig begründet werden, damit nicht der Eindruck von Willkür entsteht.

Seminararbeiten

Seminararbeit zum Thema „Wie erstelle ich eine Seminararbeit?“

Bitte werfen Sie einen Blick in die Arbeiten.

Beachten Sie, dass nicht (wie im G8) alle Schüler „freiwillig“ das Seminarfach gewählt haben, da ein ganze Klasse an dem Experiment teilgenommen hat.

Vielen Dank!