

8 Kodeverkettungen

Anwendungsfelder stellen hohe Anforderungen, wie

- Satellitenkommunikation, z. B. DVB, DVB-S2, DAB, ...
- Mobilkommunikation, WLAN, ...
- Speichersysteme, z. B. CD, DVD, MP3, ...
- Zuverlässigkeit, z. B. Programmcode, komprimierte Daten, ...

Forderung

Gleichzeitige Korrektur von statistisch verteilten Einzelfehlern und langen Bündelfehlern

Realisierung

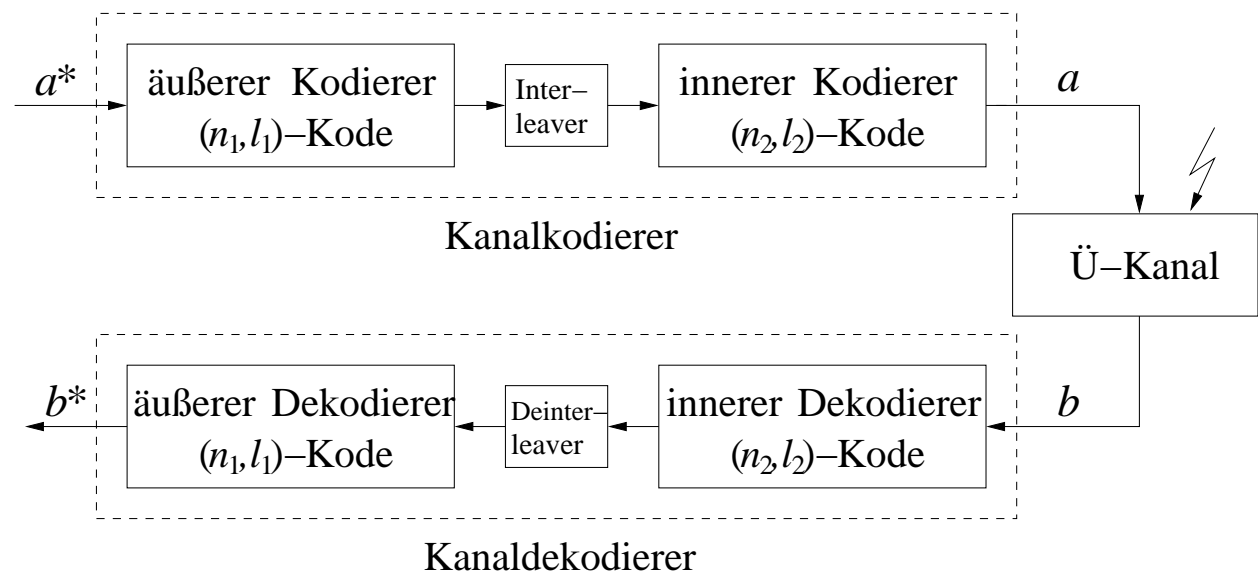
- Konstruktion leistungsfähiger, *kurzer* Codes mit Hilfe von (häufig komplizierten) algebraischen Strukturen
Ziel: Maximierung der minimalen Distanz
- Serielle Verkettung von Block-, blockfreien Codes unter Ausnutzung ihrer Leistungsfähigkeit
(FK- mit FK-Kode, FE- mit FK-Kode)
→ Separate Dekodierer sind weniger komplex; Codes werden *länger*, leistungsfähiger, aber nicht komplexer, beeinflusst von der Wahl eines geeigneten Interleavers (maximiert Distanz)
- Verbesserung des Dekodierungsverfahrens
→ iterative Dekodierung (näherungsweise ML-Umsetzung)
 - *Turbo Code* = Parallele Verkettung von Faltungskodes
 - Parallele/serielle/ohne Verkettung von Block-, blockfreien Codes
→ Zufallskodes \implies SHANNON-Grenze

8.1 Serielle Verkettung

Prinzip erstmals von FORNEY 1966 publiziert

Kodeverkettung in zwei Schritten:

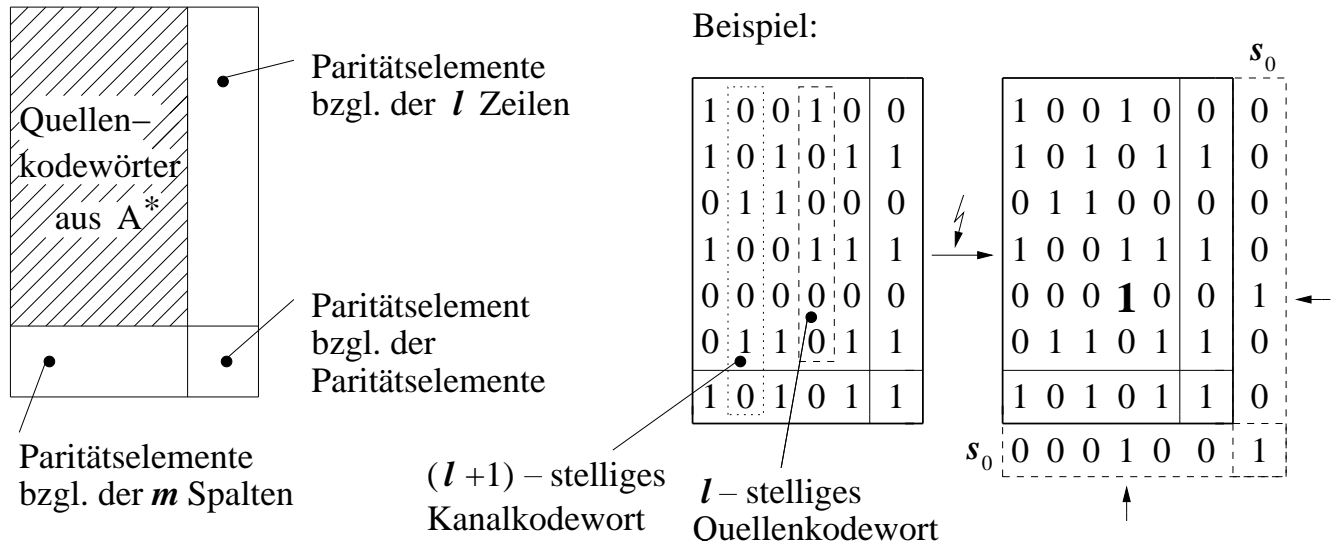
- äußere Kodierung
- innere Kodierung



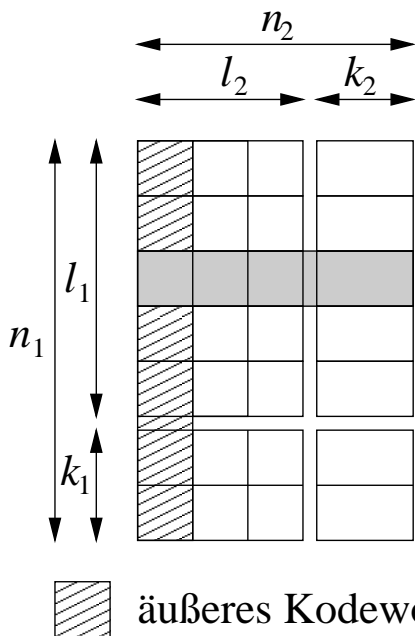
Wichtig:

Anwendung von Interleaving zur Distanz- und damit Leistungserhöhung

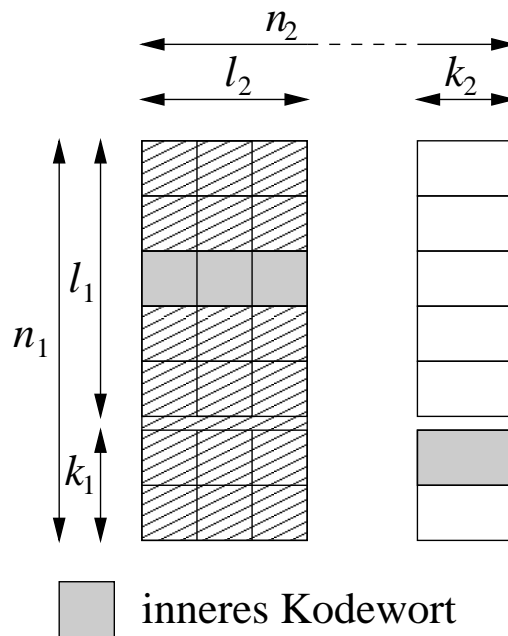
Einfachste Kodeverkettung: zweidimensionaler Paritätskode [9]
(Kreuzsicherungsverfahren)



Äußerer Kode: $u_j \in GF(2)$



Äußerer Kode: $u_j \in GF(2^{l_2})$



Bedingung für $u_j \in GF(2^{l_2})$:

wenn Kodewortelemente des äußeren Codes aus $GF(2^{k_1=l_2})$ sind (RS-Codes), dann müssen bei einem *inneren binären Blockcode* genau l_2 (oder ein Vielfaches von l_2) Kodewortelemente aus $GF(2)$ sein \rightarrow aus Synchronisationsüberlegungen und Verzögerungsbeschränkungen.

Diese Bedingung ist problemlos mit verkürzten Codes erfüllbar.

Ein *innerer RS-Code* sollte dasselbe k_1 haben.

Ein *innerer Faltungskode* wandelt die Elemente lediglich in Binärsequenzen.

Der verkettete Code ist ein $(n_1 \cdot n_2, l_1 \cdot l_2)$ **Produktcode**:

- **Koderate:** $R = R_1 \cdot R_2$
- **Minimalabstand:** $d_{min} \geq d_1 \cdot d_2$

Beispiel:

(15, 9)RS-Code über $GF(2^4)$ mit (7, 4)HAMMING-Code

Vergleich mit nichtverketteten Code gleicher Koderate:

(21, 7)RS-Code_{verkürzt} über $GF(2^5)$

d_{min}, f_k, f_b ?

Praktische Anwendungsbeispiele

NASA-Standard für Satellitenkommunikation (1987, 1998)

- **Äußerer Kode:**

(255, 223)**RS-Kode** über $GF(2^8)$

mit $M(x) = x^8 + x^7 + x^2 + x + 1$ und $g(x) = \prod_{j=1}^{143} (x - \alpha^{11j})$

soft-decision Dekodierung mit BERLEKAMP-MASSEY-Alg.

- **Kodespreizung:** helical Interleaving

(Blockinterleaving I-Tiefe 5 mit hard-decision Dekodierung)

- **Innerer Kode:**

$(7, \frac{1}{2})$ **Faltungskode** erzeugt mit $G = \begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$,

hard-decision Dekodierung mit VITERBI-Algorithmus (auch 3-Bit-Quantisierung)

—→ Mit Turbokode vergleichbarer Koderate Kodierungsgewinne größer 1 dB!

—→ 2007: Bei begrenzter Dekodierungsverzögerung (Sprachkommunikation, Speicher, ...) klassischen Kodes unschlagbar!

Weitere Anwendungen für RS-Faltungskode-Verkettung

- **Digital Video Broadcasting** (DVB-Standard, 1994)
 - DVB über Satellit (und Terrestrische Ausstrahlung):
 - Äußerer Kode: (204, 188)RS-Kode über $GF(2^8)$
 - Kodespreizung: Faltungsinterleaving
(I-Tiefe 12, Basisverzögerung D17)
 - Innerer Kode: $(7, \frac{1}{2})$ Faltungskode mit $R_p = \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{7}{8}$
3-Bit-Quantisierung mit VITERBI-Algorithmus
 - DVB über **K**abel verzichtet auf inneren Kode, weil Kabelnetze – im Gegensatz zu Satellitenstrecken – eine wesentlich höhere Übertragungsqualität gewährleisten.
- DVB-S2: Serielle Verkettung von BCH- und LDPC-Kode (Herbst 2005), auch in DVB-T2 (frühestens 2012)
- **Mars Pathfinder** mission communication (1997)
 - Äußerer Kode: (252, 220)RS-Kode über $GF(2^8)$
 - Kodespreizung: Blockinterleaving (I-Tiefe 5)
 - Innerer Kode: $(15, \frac{1}{6})$ Faltungskode
Gewinn von etwa 2 dB geg. NASA-Standard

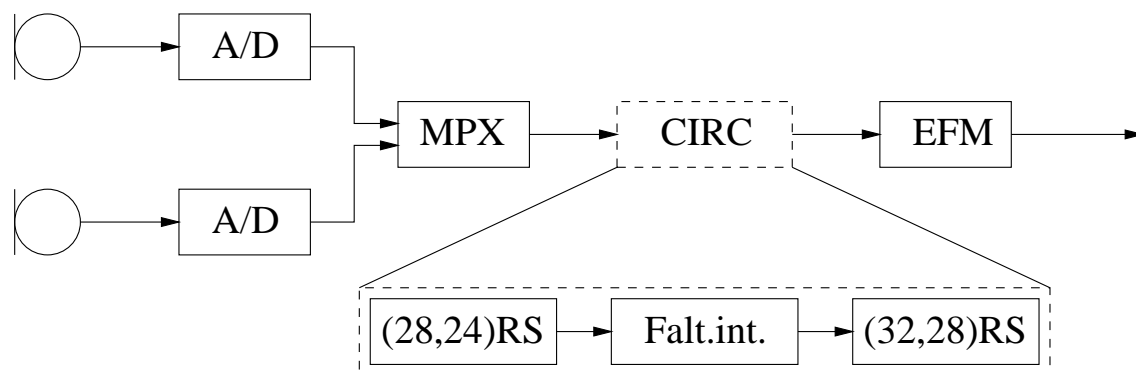
Audio-CD (1980)

Äußerer Kode: (28, 24)RS-Kode über $GF(2^8)$

Kodespreizung: Faltungsinterleaving
(I-Tiefe 28, Basisverzögerung D4)

Innerer Kode: (32, 28)RS-Kode über $GF(2^8)$

Vereinfachtes Schema der Audio-Aufzeichnung:



CIRC – Cross Interleaved REED-SOLOMON-Kode

EFM – Eight to Fourteen Modulation

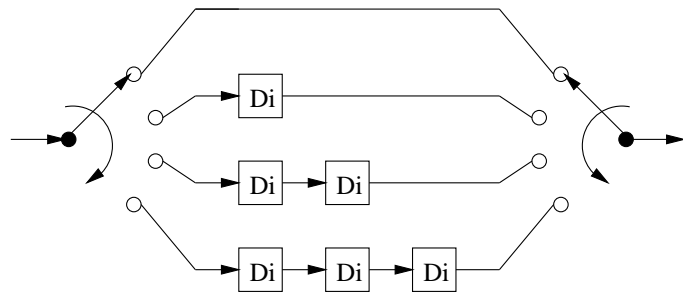
DVD (1995)

Äußerer Kode: (182, 172)RS-Kode über $GF(2^8)$

Kodespreizung: Blockinterleaver (I-Tiefe 192)

Innerer Kode: (208, 192)RS-Kode über $GF(2^8)$

Faltungsisinterleaving



- Maximale Verzögerung eines äußeren Kodewortes

$$\max_V = (I - 1) I \cdot D + n_1$$

- Minimale Verzögerung *zwischen* beliebigen Elementen eines äußeren Kodewortes

$$n_1 = I \cdot D : \min_V = I - 1$$

$$n_1 = I : \min_V = I \cdot D$$

- rekonstruierbare Bündelfehler

– Innerer Kode: Faltungskode ($n_1 = I \cdot D$)

$$f_b \leq f_k \cdot \frac{\min_V + 1}{n_1} \cdot n_2 = f_k \cdot \frac{1}{D} \cdot n_2 \quad \text{mit} \quad n_2 \approx \frac{n_1 \cdot k_1}{R_2}$$

– Innerer Kode: Blockkode (RS-Kode) ($n_1 = I$)

$$f_b \leq f_k \cdot \frac{\min_V}{n_1} \cdot n_2 \cdot k_1 = f_k \cdot D \cdot n_2 \cdot k_1$$

bzw.

$$f_b \leq \rho \cdot \frac{\min_V}{n_1} \cdot n_2 \cdot k_1 = \rho \cdot D \cdot n_2 \cdot k_1$$

Beispiele

- **DVB-Standard** $n_1 = I \cdot D$

$(204, 188)$ RS $\rightarrow I12, D17 \rightarrow (7, \frac{1}{2})$ Faltungskode

$$\max_V = 11 \cdot 12 \cdot 17 + 204 = 2448$$

(verteilt auf $\frac{2448}{204} = 12$ äußere KW)

$$\min_V = 11$$

($\approx \frac{1}{17}$ äußeres KW zwischen 2 Elementen)

$$f_b \leq 7 \cdot \frac{12}{204} (204 \cdot 8 + 6) \cdot 2 = 1348,94 \text{ Bit} \approx 168 \text{ Elemente}$$

- **Audio-CD** $n_1 = I$

$(28, 24)$ RS $\rightarrow I28, D4 \rightarrow (32, 28)$ RS

$$\max_V = 27 \cdot 28 \cdot 4 + 28 = 3052$$

(verteilt auf $\frac{3052}{28} = 109$ äußere KW)

$$\min_V = 28 \cdot 4 = 112$$

(4 äußere KW zwischen 2 Elementen)

$$f_b \leq 4 \cdot 4 \cdot 32 \cdot 8 = 4096 \text{ Bit} \quad (\rho = 4)$$

$$\text{Ist: } f_b \leq 4 \cdot 4 \cdot 588 \text{ Bit} = 9408 \text{ Bit} \cdot 0,3 \mu\text{m/Bit} = 2,8 \text{ mm}$$

Mobilfunk (GSM-Standard) (1992)

- Quellenkodierung des Sprachsignals:

Blockcode von $l = 260 \text{ Bit}$

- Kanalkodierung:

Äußerer Kode: CRC-Kode

Innerer Kode: $(5, \frac{1}{2})$ Faltungskode mit $G = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \end{pmatrix}$

Kodespreizung: Blockinterleaving (I-Tiefe 8)

Schematische Darstellung von $l = 260 \rightarrow n = 456$:

260 Bit		
---------	--	--

Quellenkode

50	132	78
----	-----	----

50+3

CRC-Kode

53	132	4
----	-----	---

Faltungskode

189	189
-----	-----

378	78
-----	----

456 Bit

Kanalkode

→ **UMTS-Standard** (2000) (u. a. CRC-, $(9, \frac{1}{2})$ Falt.kode mit $G = (561_8, 753_8)$; auch Turbokode mit $G = (1, \frac{15_8}{13_8})$)

Für die Sprachübertragung werden Faltungskodes wegen ihrer kleineren Dekodierungsverzögerung gegenüber Turbokodes auch weiterhin genutzt!

8.2 (Parallele) Verkettung und iterative Dekodierung

1993 mit *Turbo Code* [18] Durchbruch in Richtung SHANNON-Grenze geschafft

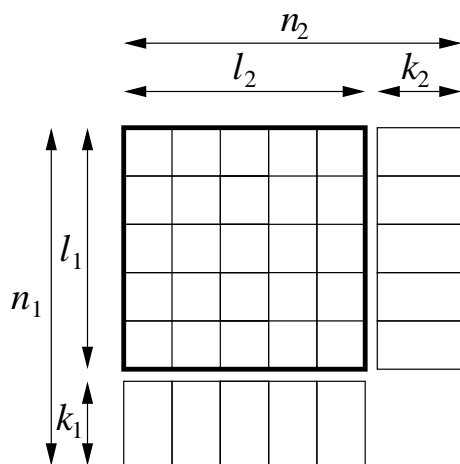
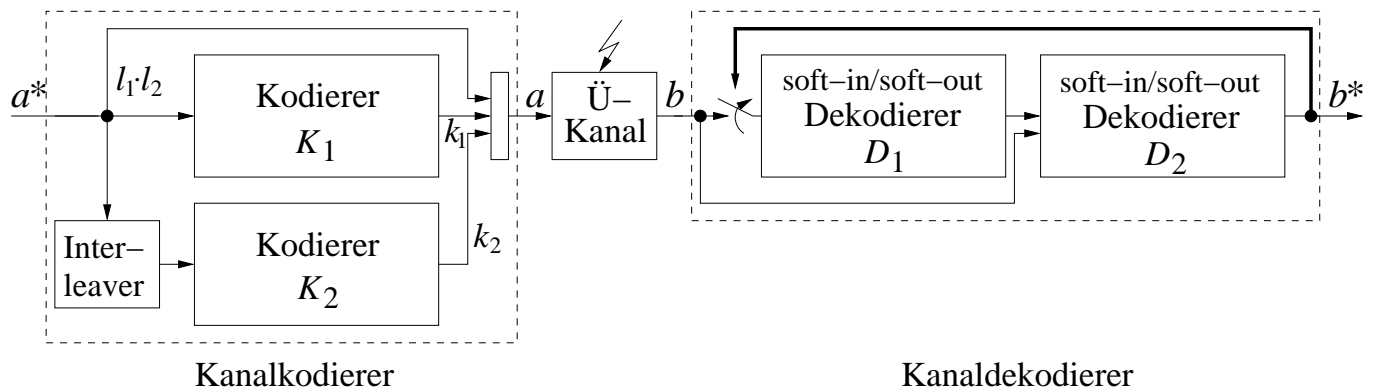
Turbo Code – **parallele Verkettung** von Faltungskodes
 + **Zufallsinterleaver** zwischen Faltungskodes
 + **große Kodewortlänge** → Zufallskode
 + **Iterative Dekodierung** → ML Leistungsfähigkeit

Prinzip bereits 1962 durch GALLAGER vorgestellt, auch 1979 rückgekoppelte Dekodierung konzeptionell erwähnt, 1993 (fast gleichzeitig) für die Dekodierung von Produktkodes aufgegriffen

- Berechnung von Zuverlässigkeitsinformation für geschätzte Informationsbits → soft-in/soft-out Dekodierer, soft-out[put] Werte sind soft-in[put] Werte des nächsten Dekodierers
- mehrere Iterationsstufen
 → Reduzierung der Dekodierungskomplexität durch Verkettung einfacher Komponentenkodes bei sehr guten Kodierungsgewinnen

Im Weiteren: parallele/serielle Verkettung von mindestens zwei binären, einfachen, systematischen/nichtsystematischen, gleichen/nichtgleichen Komponentenkodes (Block-, blockfreien Kodes)

Rätselhaftes Phänomen, warum diese schlechten Kodes (aus Sicht von d_{min}) bei kleinem SNR durch iterative Dekodierung so hervorragend dekodiert werden können [11].



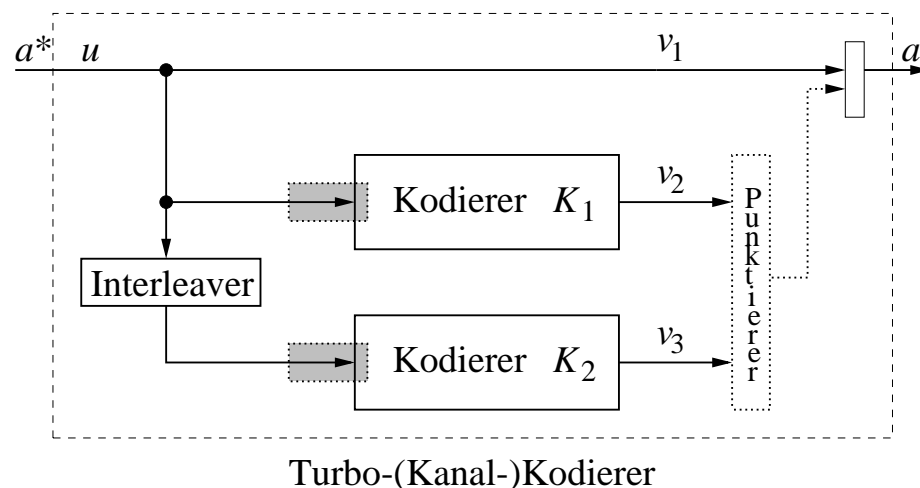
Koderate:
$$R = \frac{1}{\frac{1}{R_1} + \frac{1}{R_2} - 1}$$

(besser im Vergleich zu serieller Verkettung, da die Kontrollbits nicht geschützt sind)

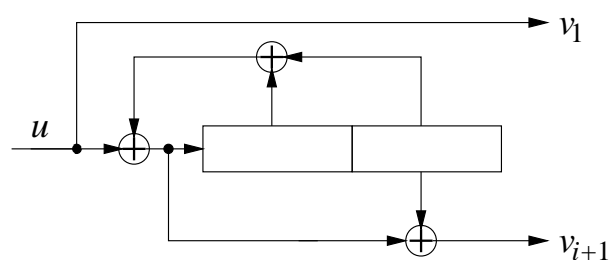
Minimalabstand:
$$d_{min} \geq d_1 + d_2 - 1$$

(schlechter im Vergleich zu serieller Verkettung)

Iterative Dekodierung bei paralleler Verkettung von rekursiv systematischen Faltungskodierern, *Turbo Code* [18]: ⁸



Komponentenkodierer K_i :



- linearer systematischer Blockcode (Informationsfolge und zwei redundante Folgen) \rightarrow Vorteil für Koderate: $R \approx \frac{1}{3}$
 \rightarrow „Vorteil“ für Rekonstruktion: Ergebnis ist immer ein b^*
- Terminierung der Komponentenkodes möglich
 (Tail-Biting bevorzugen)
- Punktierung $\rightarrow R_p = \frac{1}{2}$
 (im Vergleich zu Faltungskodes sind für parallel verkettete

⁸ Closing in on the perfect code. IEEE Spectrum, March 2004.

Kodes keine optimalen Punktierungen bekannt)

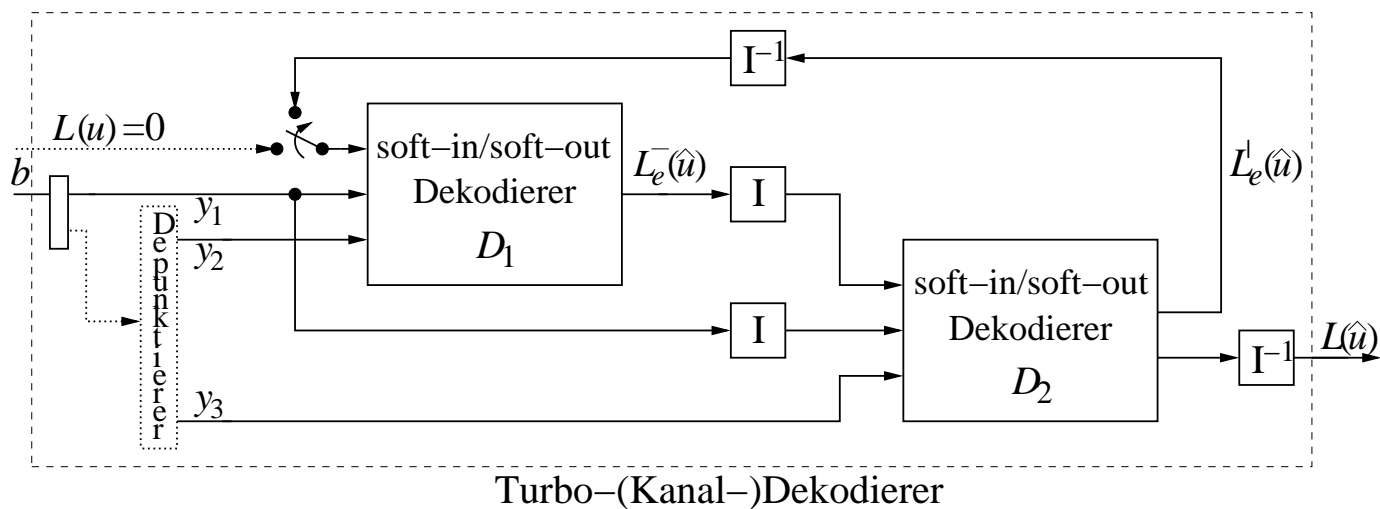
Bisher: Punktierung nur der redundanten Bits

Neu: Punktierung auch von systematischen Bits (bis zu 50%)
—→ zeigt Vorteile bei den Distanzeigenschaften und damit bei der Rekonstruktion

—→ Nachteile bei der Zahl der Iterationen [29];

Punktierung nicht unabhängig vom Interleaver

- Interleaver (Block-, Randominterleaving) dient der Maximierung der minimalen Distanz
 - bestimmt Leistungsfähigkeit des Turbokodes
 - wächst mit Größe der Informationsfolge ($l \leq 2^{16}$):
 - SHANNON's Theorie zeigt, dass größere Blöcke besser sind, weil das Gesetz der großen Zahlen es weniger wahrscheinlich macht, dass atypische Rauschereignisse in einem Block großer Länge n ($\approx 3l$) geschehen.
 - Mit der Erhöhung von n reduziert sich die Zahl von Codewörtern kleinen Gewichts.



• soft-in/soft-out Dekodierer

- (modifizierte) MAP Dekodierung (Original [17])
- aufwandsgünstigere (modifizierte) SOVA Dekodierung:

$$D_{t+1}^\sigma = \min_{\forall \sigma' \sigma} \left\{ D_t^{\sigma'} + \underbrace{d_{(E)t}^{\sigma' \sigma}}_{\text{iterationsunabhängig}} - \underbrace{x(t) \cdot \frac{L_e^l(\hat{u}(t))}{2}}_{u(t) \in \{0, 1\} \rightarrow x(t) \in \{+1, -1\}} \right\}$$

Mit Kenntnis der wahrscheinlichsten Kodefolge *und* $L(\hat{u}(t))$:

$$L_e^-(\hat{u}(t)) = L(\hat{u}(t)) - y_1(t) - L_e^l(\hat{u}(t)) \quad (t = 0, 1, \dots, n - 1)$$

(1. Iteration: $L_e^l(\hat{u}(t)) = L(u(t)) = \mathbf{0}$)

$$L_e^l(\hat{u}(t)) = L(\hat{u}(t)) - y_1(t) - L_e^-(\hat{u}(t)) \quad (t = 0, 1, \dots, n - 1)$$

Nach z. B. τ_{max} Iterationen:

$$L(\hat{u}(t)) = y_1(t) + L_e^-(\hat{u}(t)) + L_e^l(\hat{u}(t))$$

$$\hat{u}(t) = \frac{1 - \text{sign} L(\hat{u}(t))}{2} \quad (t = 0, 1, \dots, l - 1)$$

- nach erster Iteration noch keine Ausgabe einer Informationsfolge b^* (noch „Unabhängigkeit“ der Dekodierer)
- Dekodierungsergebnisse: korrekte/falsche Dekodierung
- Bisher: Abbruch nach $\tau_{max} = \underline{6} \dots 18$ Iterationen

Neu [29]: mit zusätzlicher Punktierung von systematischen Bits [partially systematic turbo codes] bis zu 40 Iterationen und mehr möglich (abhängig von Punktierungszahl), aber: die meisten Empfangsfolgen sind nach wenigen Iterationen fehlerfrei;

Stopkriterium für Zahl der Iterationen über Auswertung der extrinsischen Information (Stop, wenn mittlere Zuverlässigkeiten beider Dekodierer sich in zwei nachfolgenden Iterationen kaum noch verändern), maximal nach τ_{max} Iterationen

→ Auswertung von EXIT [EXtrinsic Information Transfer] Charts

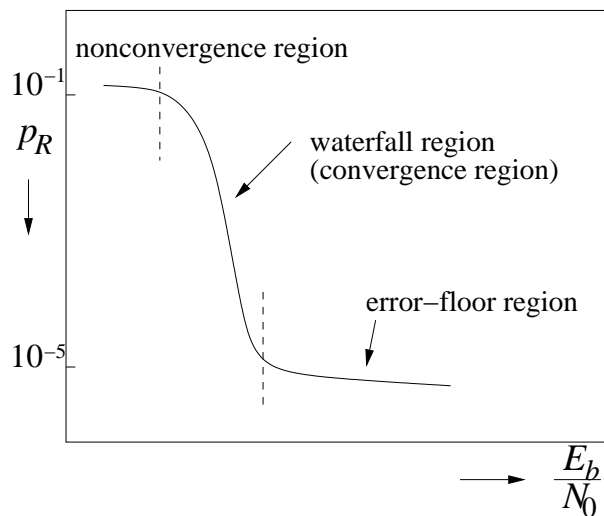
- **Leistungsfähigkeit**

mit ($K \leq 5$, $R_p \approx \frac{1}{2}$) und BPSK ist Leistung innerhalb 0,5 dB der SHANNON-Grenze ($R = \frac{1}{2} : \frac{E_b}{N_0}_{grenze} = 0,19$ dB) möglich:

$$p_R \approx 10^{-5} \quad \text{für} \quad \frac{E_b}{N_0} < 0,5 \text{ dB}$$

→ kleine Blocklängen und Begrenzung der Zahl der Iterationen können leicht zu einer Verschiebung von 1 dB führen

Typisches Verhalten von parallel verketteten Turbokodes:



Nach waterfall Bereich wird ein „Knick“ bei $p_R \approx 10^{-5}$ im Verhalten deutlich, ab da sinkt p_R nur noch wenig: error-floor. Ursache sind Kodewörter kleinen Gewichts, hauptsächlich ein Problem des Interleavers (Kodewörter hohen Gewichts führen zu geringerem error-floor).

Alternativen:

- Punktierung auch systematischer Bits (Erhöhung des Kodewortabstandes, weniger Punktierung der systematischen Bits „besser“ für waterfall Bereich aber „schlechter“ für error-floor Bereich und umgekehrt – im Vergleich zu herkömmlichen systematischen Turbokodes besser –)
- serielle Kodeverkettung (vergleichbares Leistungsverhalten ohne Knick, sogar bei $k = 2$, parallel bei $k = 4$)
- Kodeverkettung von Turbokode mit äußerem Blockcode, z. B. BCH-Kode, zur „Auflösung“ des error-floor

- **Nachteile:**

Komplexität wächst mit Zahl der Iterationen, kaum Parallelisierung möglich, Turbokodes nicht beliebig dimensionierbar (Kodeparameter!)

Anwendungen

- Turbokodes für Weltraum(Satelliten)kommunikation
 - $R = \frac{1}{3}$ durch parallele Verkettung von zwei $(5, \frac{1}{2})$ rekursiv systematischen Faltungskodierern (RSC)
 - $R = \frac{1}{4}$ durch parallele Verkettung von $(5, \frac{1}{3})$ und $(5, \frac{1}{2})$ RSC

SMART-1: erste Raumsonde mit Turbokode-Anwendung (2003-2006)
- Turbokodes für 3. Mobilfunkgeneration (UMTS, 2001), $G = (1, \frac{158}{138})$; Standardisiert durch 3rd Generation Partnership Project (3GPP) in Verkettung mit CRC
- Turbokode für 4. Mobilfunkgeneration (LTE, LTE Advanced, 2011/2013) in Verkettung mit CRC
- DVB-RCS [Return Channel over Satellite], $(4, \frac{1}{3}, \dots, \frac{6}{7})$ RSC
- DVB-SH [Satellite to Handheld] (multimedia services over digital hybrid satellite/terrestrial broadcasting networks to handheld terminals) 2008, Verkettung $(255,191)$ RS- mit Turbokode⁹
- :

⁹http://www.dvb-h.org/PDF/a120.tm3731r5.ssp252r9f.DVB-SH_implementation_guide.pdf