

Codierung, Chiffrierung, Interleaving, Modulation

„Gut gekörnt ist halb gebohrt – die Bandbreite verdoppelt sich nur alle 100 Jahre“

Dieses Kapitel behandelt die Körnung, Auslegung und Dimensionierung der Satellitenübertragung, der Weg von der Quelle (Sprache, Daten, Bewegtbild) bis zur Senke (das Ohr, das Auge, der Computer); diese Kette ist in Abb. 4.1 dargestellt:

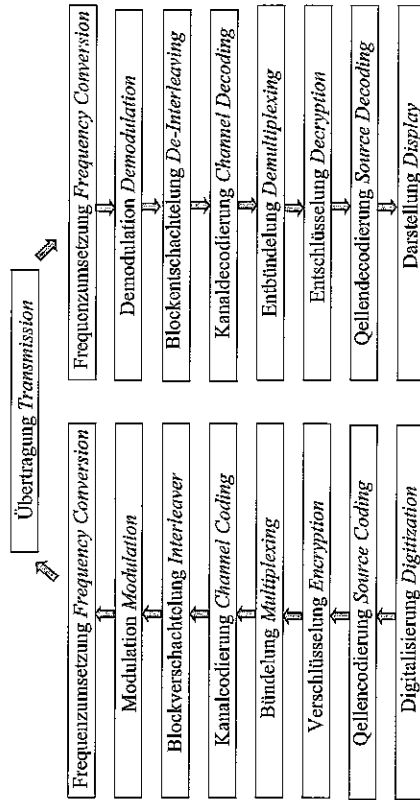


Abb. 4.1 Die Sequenz der Signalverarbeitung und -übertragung

Die Digitalisierung wird vorgenommen, weil das Signal nur in der digitalen Form quellcodiert und komprimiert werden kann.

Die Quellcodierung ist vorteilhaft, um das Signal darzustellen und zu komprimieren, damit es weniger Bitrate und Bandbreite bei der Übertragung benötigt.

Die Verschlüsselung ist für den Datenschutz notwendig, im Allgemeinen und bei Funkstrecken, terrestrisch oder via Satellit besonders.

Die Bündelung erlaubt die effizientere Übertragung mehrerer Quellen auf einem Hochfrequenzträger anstatt die Quellsignale einzeln zu übertragen.

Die Kanalcodierung dient dem Fehlerschutz auf der Funkstrecke; durch zusätzliche Code-Bits können dB an physikalischer Leistung eingespart werden.

Die Blockverschachtelung ist ein Mittel zur Behebung von Signalausfällen, zum robusten Fehlerschutz insbesondere auch beim Ausfall einer zusammenhängenden Bitfolge, die die Kanalcodierung nicht korrigieren kann.

Die Modulation ist nötig, weil das unmodulierte Signal in der Tonfrequenz nicht über weite Entfernungen übertragen werden könnte.

Die Frequenzumsetzung konvertiert das Signal in die für die Funkübertragung geeignete Hochfrequenz und dann wieder zurück ins Basisband zum Nutzer.

Die Kette von der Quelle bis zur Sendeantenne ist in Abb. 4.2 gezeigt. Dabei kann die Verschlüsselung, anstatt, wie im Bild gezeigt, auf das Summensignal zu wirken, auch vorteilhaft auf die Einzelsignale individuell angesetzt werden.

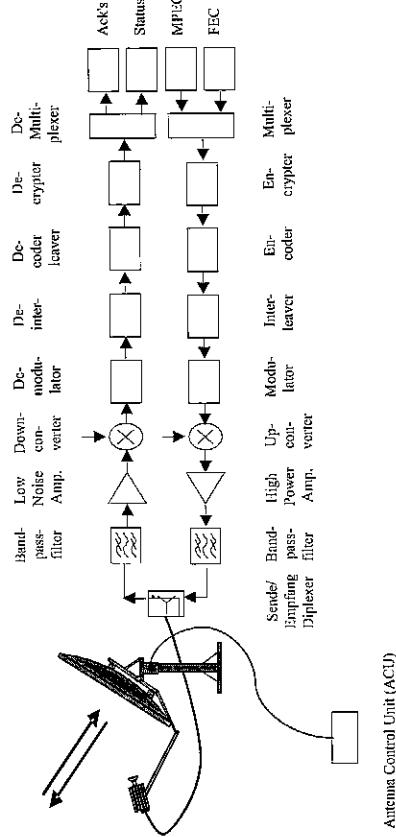


Abb. 4.2 Die Kette von der Quelle bis zur sendenden Erdfunkstelle und zurück, mehrere Kanäle gemultiplext

4.1 Digitalisierung – die Nyquist Rate

In der ersten Stufe werden die Signale $u(t)$ digitalisiert. Hierzu werden sie mit der Nyquist Rate abgetastet. Jeder Abtastwert wird als Zahl übertragen, zum Beispiel mit $m = 8$ bit, also 256 Stufen. Das resultierende Quantisierungsrauschen n und die Signalleistung s betragen

$$n = \frac{1}{T} \int_{-\frac{T}{2}}^{+\frac{T}{2}} u(t)^2 dt = \Delta \frac{u^2}{(12R)} \quad (4.1)$$

wobei $\Delta u =$ Spannungsquantisierung über dem Widerstand R und $T =$ Nyquistperiode; und

$$s = (k^2 - 1) \cdot \frac{\Delta u^2}{(12R)} \quad (4.2)$$

mit $k =$ Zahl der Quantisierungsintervalle, so dass

$$\frac{s}{n} = k^2 \quad (4.3)$$

► Nach Nyquist muss die Zahl der Abtastwerte das Doppelte der höchsten Frequenz $f_{\max}$ des Signales s betragen, um keine Information zu verlieren:

$$k = 2f_{\max}$$

Telefonsprache mit $f_{\max} = 4$ kHz wird mit 8000 Werten pro Sekunde abgetastet.

Für $m = 8$ Bit pro Abtastwert wird die Bitrate zu 8 Bit 8000 Werten pro Sekunde, also 64 kbit/sec.

Mit $2^8 = 256$ ist $s/n = (2^8)^2 = 65\,536$ oder 48 dB. In dB gilt

$$S - N = 6m \quad (4.4)$$

mit $m =$ Anzahl der Bit pro Abtastwert, so dass

$$m = 8 \quad 10 \quad 12 \quad 14 \quad 16$$

$$S - N = 48 \text{ dB} \quad 60 \text{ dB} \quad 72 \text{ dB} \quad 84 \text{ dB} \quad 96 \text{ dB}$$

Die Tabelle zeigt einige in Europa, den USA und Japan gängige Bitraten:

Tabelle 4.1 Gängige Bitraten in Europa, Amerika und Japan

Name	Abk.	EU	USA	Japan
1 Telex Speed	CCITT-7	50 b/s	50 b/s	50 b/s
2	V.21	300 b/s	300 b/s	
3	V.22	1,2 kb/s		
4 Voice Speed	LPC10	2,4 kb/s	2,4 kb/s	
5	G.729	8 kb/s	8 kb/s	
6		9,6 kb/s		
7 D-Kanal	G.728	16 kb/s		
8	G.721	32 kb/s		
9 Digital Signal Level 0	DS 0/V.90		56 kb/s	56 kb/s
10 A-Kanal	G.711	64 kb/s		
11 Integrated Services Dig.Netw.	ISDN	144 kb/s		
12 PCM-Multiplex	DSMX	384 kb/s		
13		512 kb/s		
14 DS-1	T1		1,544 Mb/s	1,544 Mb/s
15 PCM 30	E1	2,048 Mb/s		
16 DS-2	T2		6,312 Mb/s	6,312 Mb/s
17 Multiplexed E1	E2	8,448 Mb/s		
18	J3			32,064 Mb/s
19 PCM/DSMX 34	E3	34,368 Mb/s		
20 DS-3	T3		44,736 Mb/s	

ding Law) wieder expandiert wird. Amplituden-Compandierung wird bei AM und FM angewandt. Der erreichte Compandierungsgewinn als Funktion des Signal/Rauschabstandes $S-R$ ist:

$$CG = 0,464 \cdot (S - R) - 4,125 \text{ dB} \quad \text{für } S - R > 15 \text{ dB} \quad (4.5)$$

In der Praxis wird ein Amplitudencompandierungsgewinn von 7 bis 10 dB erzielt.

4.2.1.2 Frequenz-Compandierung

Im Gegensatz zum Amplituden- macht der Frequenz-Compandierer von der Tatsache Gebrauch, dass tiefe Vokallänge und hohe Konsonantenklänge nicht gleichzeitig vorkommen und komprimiert das Frequenzband. In praxi werden bis zu 60% des Basisbandes gepresst. Dass ergibt ca. 2 kHz pro Sprachkanal, statt 3,4 kHz. Damit werden im *Companded Single Sideband-Suppressed Carrier*-Betrieb im 40 MHz-Transponder, der mit FDM/FM/FDMA 500 und mit PCM/QPSK/TDMA 1 000 Kanäle übermittelt, 18 000 Kanäle übertragen. Der Compandierungs-Gewinn fusst auf der reduzierten Hochfrequenzbandbreite und damit dem proportional reduzierten Rauschleistungsanteil:

$$CG = 10 \log \frac{b_{\text{nicht-reduziert}}}{b_{\text{reduziert}}} \text{ [dB]} \quad (4.6)$$

In der Praxis wird ein Frequenzcompandierungsgewinn von 3 dB erzielt.

4.2.1.3 Begrenzer

Eine billigere Methode der Amplitudenkompression ist, die Signalspitzen abzuschneiden (s. Abb. 4.3), um den dynamischen Bereich zu begrenzen. Im Gegensatz zur Compandierung, die das Signal nicht degradiert, entsteht bei dieser nichtlinearen Begrenzung (*Peak Clipping*) Intermodulation. Um diese klein zu halten, muss die Begrenzung klein gehalten werden.

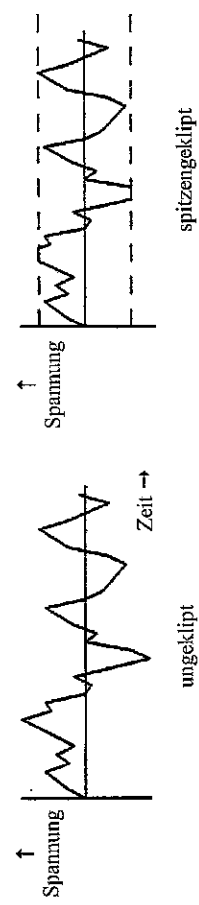


Abb. 4.3 Das Prinzip des Peak Clipping

Die Begrenzung der Amplitude wird auch verwendet, um die Auswirkung eines Störers im Rahmen zu halten (siehe „*Limiter*“ in Kap. 11).

Tabelle 4.1 Fortsetzung

21	Optical Carrier Level 1	OC-1	-	51,840 Mb/s	-	97,728 Mb/s
22		J4	-	-	-	-
23	Optical Carrier Level 2	OC-2	-	103,680 Mb/s	-	-
24	PCM/DSMX 140	E4	139,264 Mb/s	-	-	-
25	Optical Carrier Level 3	STM-1	-	155,520 Mb/s	-	-
26	DS-4	T4	-	274,176 Mb/s	-	-
27		J5	-	-	-	400,352 Mb/s
28		STM-3	466,56 Mb/s	-	-	-
29	PCM/DSMX 560	E5	560,0 Mb/s	-	-	-
30	Opt. Carrier Lev. OC-4	STM-4	622,2 Mb/s	622,2 Mb/s	-	-
31		STM-8	1,244 Gb/s	-	-	-
32	Opt. Carrier Lev. OC-5	STM-9	-	1,5 Gb/s	-	-
33		STM-16	-	2,48832 Gb/s	-	-
34	Opt. Carr. Lev. OC-192	STM-64	-	10 Gb/s	-	-

4.1.0.1 Aliasing

Aliasing entsteht, wenn ein Signal unter der Nyquist Rate abgetastet wird. Dabei gehen alle höherfrequenten Signalanteile verloren und werden empfangsseitig falsch interpretiert.

Beispiel 1: Digitales Audio wird mit 48 kb/s abgetastet. Die Schwingung höchster Frequenz, die korrekt wiedergegeben wird, ist 24 kHz. Ein 30 kHz Ton wird zum 18 kHz Ton. Dies ist eine hörbare, lästige Verzerrung. Ein gehörter 18 kHz Ton kann von einer 18 kHz Signalkomponente herrühren, oder aber auch von einem 30-kHz-Signalanteil. Der Ton ist 18 kHz *alias* 30 kHz.

Beispiel 2: Ein alter Wildwestfilm zeigt einen fahrenden Wagen mit 25 Bildern pro Sekunde. Die Speichenräder drehen sich schneller als 25-mal pro Sekunde. In der Filmwiedergabe drehen sie sich rückwärts – eine Fälschung, weil die Bildfolge unter der Nyquist Rate der Raddrehung liegt.

4.2 Quellencodierung

4.2.1 Compandierung

Zur besseren Nutzung der (kostbaren) Satellitenleistung und des (endlichen) Frequenzspektrums verdichtet (komprimiert) man Amplitude und Frequenzhub der Signale.

4.2.1.1 Amplituden-Compandierung

Die Störung eines Signals wird reduziert, wenn seine Amplitude vor der Übertragung komprimiert und danach nach der inversen Gesetzmässigkeit (*Compan-*

werden, wird aber von dem dominierenden Sprachsignal „maskiert“ und subjektiv in den Hintergrund verdrängt.

Der *Center Clipper* wird auch in digitalen Systemen zur Unterdrückung von Brummtönen eingesetzt.

Neben dem *Center Clipper* wurde früher noch die Telefonkreisabschaltung² (*Speech Detection*) und das Echoauslöschungsverfahren³ (*Echo Cancellation*) verwendet.

4.2.2 Sprachcodierung

Quellencodierung eindimensionaler Signale (Sprache) wird mit Verfahren wie *Discrete Cosine Transform*, *Waveform Coding* und *Vector Coding* gemacht. Da Sprache noch für lange Zeit ein wesentlicher Verkehr ist, ist es wichtig, sie mit so wenig Aufwand wie möglich zu übertragen. Der Aufwand bei der Funkübertragung drückt sich in Sendeleistung C und Bandbreite B aus; die Sendeleistung ist

$$C = E_b + 10 \log [\text{Bitrate}] + \text{const.} \quad (4.7)$$

und die Bandbreite ist proportional zur Bitrate. Folglich ist es für die Minimierung von Leistung und Bandbreite gleichermaßen wichtig, die Bitrate zu minimieren.

Im Prinzip genügen zwölf *Diphthonge*, um die menschliche Sprache zu erzeugen. Jeder *Diphthong* kann mit vier Bit dargestellt werden. Die Dauer eines *Diphthongs* ist im Mittel 10 ms; damit ergibt sich eine mittlere Bitrate von 72 bit/s für die Wiedergabe der Sprache. In praxi genügen sogar 50 bit/s, abhängig von Sprecher und Sprache.

Die so restaurierte Sprache kann blechern und unpersönlich klingen. Für die breite Akzeptanz des Telefons wird Sprechererkennung (*Talker Identification*) verlangt. Um dies dem Sprachsignal wieder hinzuzufügen, erhöht man die Minimalbitrate um den Faktor 2 bis 4, auf bis zu 300 bit/s. *Voice-Codierer (Vocoder)* mit 300 bit/s wurden der Fachwelt 1982 vorgestellt. Für das Militär entwickelte Geräte gehen ca. sechs Jahre weiter zurück. Inzwischen gibt es Entwicklungen, die im Bereich 300 bit/s ... 600 bit/s (mit *Talker Identification*) arbeiten.

Sendeleistung kann auch durch Unterbrechung der Sendung während der Sprechpausen (wenn der Andere spricht etc.) reduziert werden; man spricht etwa 50% der Zeit und hört 50% der Zeit zu, und während des Sprechens sind 20% Sprechpausen. Der Kanal ist nur 40% der Zeit aktiv. Wenn Sendeleistung nur zugeteilt wird, wenn der Kanal aktiv ist, kann 60% Leistung eingespart werden (nicht jedoch Bandbreite). Dies nutzte die COMSAT mit dem *Digital Speech Interpolation (DSI)* für Satellitenübertragung.

² Die Telefonkreisabschaltung, wenn die Gegenstelle nicht spricht, verhindert zwar ein Echo, benötigt aber schnelle Detektoren, die melden, wenn nicht gesprochen wird; häufig schneiden diese Detektoren die ersten Silben ab.

³ Die technisch beste Lösung ist die Echosubtraktion; in den ersten Millisekunden der Verbindung vermessen Plottöne Laufzeit und Dämpfung des Sprechkreises; danach kann auf beiden Seiten das gesprochene Wort, um die Laufzeit versetzt und um die Dämpfung skaliert, von dem ankommenden Signal subtrahiert und das Echo eliminiert werden.

4.2.1.4 Echo

Im klassischen Kupferkabel-Telefonnetz war das teuerste Glied die Verbindung zum Teilnehmer; deshalb legte man sie als Zweidrahtverbindung aus und wandelte sie im Teilnehmerendgerät mit Hilfe einer Gabelschaltung¹ in die Vierdrahtverbindung, die zum Betrieb von Mikrophon und Lautsprecher notwendig ist. Die Impedanz dieser Gabel konnte aber nicht an die Impedanz der Zweidrahtstrecke angepasst sein, da die Zweidrahtstrecke zu jedem Teilnehmer verschieden lang ist. So reflektierte ein Teil des ankommenden Signals zurück zum Sender; dieses Echo konnte nie ganz unterdrückt werden und war besonders bei Satellitenverbindungen lästig, weil das gesprochene Wort hörbar zeitversetzt zurückkallte.

Mit der Einführung der Halbleitertechnik wurde es möglich, dass jeder Telefonanschluss bei der Installation abgeglichen werden konnte – das Echo war eliminiert.

4.2.1.5 Der Rauschunterdrücker

Ähnlich dem Begrenzer (siehe oben) schneidet der Rauschunterdrücker ein Stück des Signals ab, hier den Spannungsbereich um den Nulldurchgang. Damit eliminiert man ein Brummen, aber auch das Echo (den Hall) von Weitverkehrsverbindungen, bei denen noch analoge Frequenzweichen im Spiel sind.

Der den Spannungsbereich um den Nulldurchgang ausschneidende Rauschunterdrücker (*Center Clipper*) lässt im Telefonkreis das Signal durch, wenn es über einem Spannungsschwellenwert liegt und stoppt es („öffnet den Schalter“; s. Abb. 4.4), wenn es darunter fällt. So wird der Zwischenbereich (Niedrigspannungsanteil) des Sprachsignals entfernt.

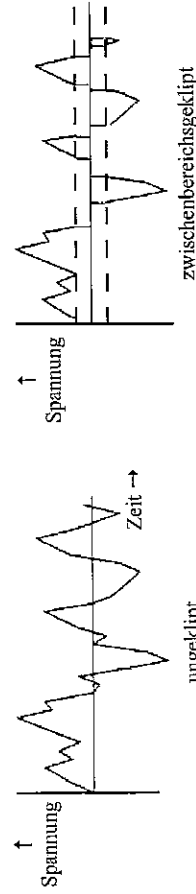


Abb. 4.4 Das Prinzip des Center Clipping

Wenn nur ein Echo ankommt, mit typischerweise einem Achtel der Leistung des Sprachsignals, und der *Center Clipper* alles unter 12,5% der Soll-Leistung herauschneidet, wird das lästige Echo unterdrückt; es kann zwar nicht ausgeschnitten

¹ Die Brückenschaltung besteht im Wesentlichen aus den zwei Spulen eines 1:1 Transformators, die eine an der Zweidrahtseite, die andere telefonseitig. Diese wird mittig abgegriffen, auf eine Impedanz geführt, die der mittleren Leitungsimpedanz entspricht, und deren Ausgang der gemeinsame Brdleiter der Vierdrahtseite ist.

Mit der digitalen Sprachverarbeitung *Continuous Variable Slope Delta-pulse-code-modulation*; CVSD) hat COMSAT ein weiteres Digitalverfahren entwickelt, in dem zusätzlich zur Pauseneliminierung die Signalprädiktion bzw. Interpolation gemacht wird, die erste Ableitung des Signals wird im Delta-Verfahren übertragen. Das CVSD wurde im INTELSAT-System eingeführt.

Tabelle 4.2 zeigt die Systemkomplexität, die Bitrate und grobe Kostenangaben für die Vocodingverfahren. Sie werden unter der Bezeichnung *Waveform Coding* zusammengefasst. Weitere Reduktionen werden durch *Vector Coding* erreicht: Das Signal wird aus dem Zeitbereich in einen höheren Bereich transformiert, zum Beispiel den Fourier-Bereich (*Fast Fourier Transform*; FFT) und den Bereich *Linear Predictive Coding* (LPC10).

Es gibt kaum ein Kostengefälle zwischen den Verfahren; bei der Auswahl des *Vocoders* entscheiden primär die Interoperabilität mit dem Partner und dann die Sprachqualität.

Tabelle 4.2 Relative Systemkomplexität, Bitrate, Kostenangaben für Vocodingverfahren

Relative Komplexität	Bitrate [bit/s]	Abkürzung	Vocoding Verfahren	Kosten [€]
1	32 000	ADPCM	<i>Adaptive Differential PCM</i>	< 100
2	16 000	CVSD	<i>Continuous Variable Slope Delta-PCM</i>	
5	9 600	P-P ADPCM	<i>Pitch-Predictive ADPCM</i>	
50	6 000	APC	<i>Adaptive Predictive Coder</i>	
50	4 800	REL P	<i>Residual Exciter Linear Predictor</i> (INMARSAT)	< 100
100	2 400	LPC-10	<i>Linear Predictive Coefficient</i>	
400	800	LPC-VEC	<i>LPC Vector Quantization</i>	
500	600	FORMANT	<i>FORMANT vocoder</i>	
600	200	V/M-QUANT	<i>Vector/Matrix QUANTization</i>	
1 000	50	Articulatory	<i>Vocal tract synthesizer; analysis and synthesis</i>	< 100

4.2.3 Videokomprimierung

Parallel zur Digitalisierung der Sprachkanäle, wobei zum Beispiel 2000 Kanäle in TDM/TDMA in der gleichen Bandbreite (36 MHz) wie 1000 analoge Kanäle in FDM/FDMA übertragen werden können, werden auch Bewegtbilder digitalisiert und zur Übertragung komprimiert.

Die Zahl der Programme nimmt stetig zu; auch hier führt Digitaltechnik zu niedriger Bitrate und so zu mehr Programmen im Kabel oder Satellitentransponder. Seit 1993 werden die so genannten MPEG-Programme eingesetzt. Nach INTELSAT-K, STAR-TV und ASIATAT hat auch ASTRA den Betrieb aufgenommen.

Der ISO-MPEG-Standard wurde von der *Motion Picture Expert Group der Internationalen Standard Organization* (ISO) definiert. Ohne digitale Kompression wären etwa

- 700 Mbit/s für die Übertragung eines Fernsehbildes notwendig⁴, etwa
- 1,6 Gbit/s für ein 16 x 9-HDTV mit 1250 Zeilen, also
- 3,2 Gbit/s für stereoskopisches HDTV⁵.

Wenn durch Komprimierung ein Fernsehbild mit 2 Mbit/s übertragen werden kann, ist der Komprimierungsgewinn also $700/2 = 350$ oder 25 dB, wenn HDTV-Stereoskopie mit 4 Mbit/s übertragen wird, ist der Komprimierungsgewinn $3176/4 = 12\,704$ oder 41 dB.

Die Digitaltechnik bietet heute bis zu 20 mal mehr Programme, bei gleichzeitig besserer Wiedergabequalität oder kleineren Heimempfangsanlagen oder einer größeren geographischen Reichweite bei gleicher Satellitensendeleistung (oder einer geschickten Kombination dieser drei Systemckwertverbesserungen), auf der Basis der Komprimierung.

4.2.3.1 Bildprädiktion und Bewegungskompensation

Die Basis von MPEG ist die Diskrete Cosinus-Transformation (*Discrete Cosine Transform* – DCT); Prädiktion und Interpolation sind das Herzstück der Kompression von Bildfolgen. Die bewährte Methode der Wittervorhersage zu sagen, dass es morgen so sein wird wie heute, trifft bei Bewegtbildern mit ähnlichem Erfolg zu. Gut 90% des Folgebildes sind unverändert – ausser bei Szenenwechseln. Folglich identifiziert man die Bildelemente, die sich geändert haben; es besteht keine Notwendigkeit, die kompletten Einzelbilder zu übertragen.

Im MPEG-Standard werden zwölf aufeinander folgende Bilder pro Rahmen (*Intra Rahmen* oder *I Rahmen*) verarbeitet. Der *Encoder* sendet dann die Information über Richtung und Ausrichtung der Änderungen im Folgerahmen. Der Decoder empfängt und gibt das erste Bild weiter und verwendet dann die anstehende Bildprädiktionsinformation, um die Bilder „4“ und „8“ zu rekonstruieren. Nach der Generierung der Bilder „4“ und „8“ werden Prädiktions- und Interpolationsalgorithmen eingesetzt, um die Bilder „1“, „2“, „3“, „5“, „6“, „7“, „9“, „10“, „11“ zu berechnen (*B-Rahmen*); dann sind die zwölf Bilder des Rahmens wiederhergestellt, obwohl nur eines (das I-Bild) übertragen wurde; die anderen elf Bilder wurden vom Decoder konstruiert.

MPEG4 maximiert die Interpolation zwischen I-Bildern und erzielt damit die niedrigsten Bitraten; MPEG2 arbeitet mit weniger interpolierten Bildern zwischen I-Bildern und ist damit besser für die Übertragung auf Funkstrecken und insbesondere auf Mobilfunkstrecken geeignet, wo auch mal I-Bilder verloren gehen können. Dieses würde dann bei MPEG-4 zum Verlust der Folgebilder bis zum nächsten I-Bild führen.

⁴ { 625 Zeilen/Bild · 625 Pixels/Zeile · 50 Bilder/s · [3 Farben/Pixel · 8 bit/Farbe + 12 bit für die Luminanz] + 2 · 2 Mbit/s für Audio } = 707 Mbit/s

⁵ { 1250 Zeilen/Bild · 704 Pixels/Zeile · 50 Bilder/s · [3 Farben/Pixel · 8 bit/Farbe + 12 bit für die Luminanz] + 2 · 2 Mbit/s für Audio } · 2 Kanäle = 3,176 Gbit/s

4.2.3.2 Codierung mit Variabler Bitrate, VBR

Bei konstanter Bitrate werden sowohl komplexe Bildelemente, die es nötig haben, als auch simple Bildelemente mit derselben Bitrate wiedergegeben, wobei bei letzteren Bits verschwendet werden. *Variable Bit Rate* (VBR) Codierung spart bis zu 40% Übertragungsbit ohne Bildqualitätsverlust. Hierzu verwendet der *Encoder* eine *Metric* der aktuellen Bildqualität (*Picture Quality Rating*; PQR).

Im Verbund mit intelligenten Multiplexern (*Statistical Muxes*), die vom Einzelsignal nur die jeweils notwendige Bitrate übertragen, ist VBR von bedeutendem Vorteil. Zehn Bilder á nominell 2 Mb/s können so mit 8 Mb/s Summenbitrate übertragen werden.

4.2.3.3 Modulation von MPEG-Signalen

In QPSK-Modulation nimmt ein 2 Mbit/s MPEG-Signal ca. 1,5 MHz Hochfrequenzbandbreite ein. In einem DTH-Transponder von zum Beispiel 27 MHz Bandbreite können so theoretisch bis zu 18 Programme als *Single-Channel-Per-Carrier* (SCPC) im Mehrträgerbetrieb angeordnet werden. Die durch den Mehrträgerbetrieb generierte Intermodulation reduziert die Anzahl jedoch auf 10 bis 12 Träger.

Deshalb bündelt man die Programme im Zeitmultiplex (*Time Division Multiplex*; TDM; *Skyplexing*) auf einen gemeinsamen Träger, der im Einträgerbetrieb mit zum Beispiel 45,71 Mbit/s im Transponder übertragen wird; mit Rate 7/8 codiert können 40 Mbit/s oder bis zu 20 MPEG-Programme (à 2 Mbit/s) abgestrahlt werden. Es können auch fünf HiFi-Programme à 8 Mbit/s oder jede Kombination von 2 Mbit/s, 4 Mbit/s, 6 Mbit/s und 8 Mbit/s-Signalen sein.

4.2.3.4 Zusammenfassung MPEG

MPEG-2 ist ein ISO-Standard, der bereits vor seiner Einführung international anerkannt wurde. Der Codier/Decodierprozess wurde so gestaltet, dass der Aufwand in die Codierung verlagert wurde und die Decodierer so einfach wie möglich sind: Der Codierer kostet z.B. 20 €, der Decodierer < 100 €. Die Signalverarbeitung dauert < 1 s.

Das MPEG-2-Verfahren beschreibt eine Reihe von Kompressions-Algorithmen und die Speicherung von Video-, Stereo-Audio- und Begleitdaten, ohne eine feste Bitrate vorzugeben. Diese kann von 1,5 Mbit/s bis über 15 Mbit/s variieren, je nach Art des Quellensignales und der geforderten Wiedergabequalität.

Da der Endnutzer für die MPEG-Übertragung in den Decoder investieren muss (es sei denn, er bezieht das Signal aus einem Kabel, in das die SMATV-Station es bereits rückkonvertiert eingespeist hat) müssen diese Programme etwas Zusätzliches bieten, um den Zuschauer zu der Investition zu bewegen. Denkbar wären, abgesehen von einer höheren Programmauswahl, *Pay-TV*, *Pay-per-View*, *Video-on-Demand*, *Interactive TV*, *Home Shopping*, 16:9-HDTV⁶ etc.

⁶ HDTV = *High Definition Television*, hoch auflösendes Fernsehen, meist im 16:9-Format

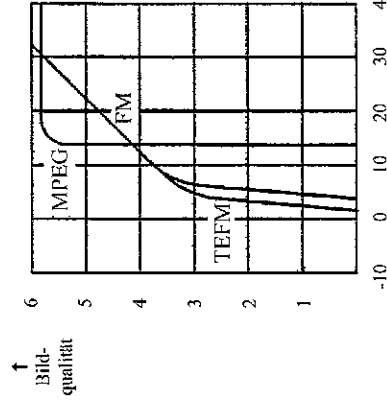


Abb. 4.5 Bildqualität von analoger (FM und Threshold Extension-FM, TEFM) und MPEG-Übertragung, gegen C-N

Einher mit der Komprimierung der Bilddaten geht die Informationsentropie aller Einzelbits: Die Bits müssen korrekt sein, dann hat das Bild hohe Qualität. Sind alle Bits korrekt, erfolgt keine weitere Bildqualitätssteigerung (s. Abb. 4.5; die Kurve flacht aus). Wird die notwendige Bitfehlerrate jedoch unterschritten, bricht die Bildqualität völlig zusammen, im Gegensatz zu der graduierlichen Verschlechterung analoger Signale.

Die MPEG-Standards können wie folgt zusammengefasst werden:

- MPEG1 VHS Qualität Video (1,5 Mbit/s); wird bei CD-ROM und DAB verwendet; seit 1993 standardisiert;
- MPEG2 Gute Qualität (2-10 Mbit/s), rückwärtskompatibel mit MPEG1; *Digital Video Broadcast* (DVB) und *Digital Versatile Disc* (DVD); seit 1994 standardisiert; das Audio im Internet, bei DARS (USA) und *Worldspace* ist der Tonkanal von MPEG2;
- MPEG4 aktueller TV-Standard mit ca. 4 Mb/s für das normale Bild und etwa 8 Mb/s für HDTV;
- MPEG5 für „Multimedia Hypermedia“ Standard PEG4 Settop Boxes
- MPEG7 wird für multimediale Anwendungen konzipiert, einschliesslich *Content Analysis*.

4.2.4 Audiokomprimierung

Für *Digital Audio Broadcast* (DAB), terrestrisch und via Satellit abgestrahlt, werden regional verschiedene Frequenzbänder verwendet:

USA, IND:	2310-2345 MHz (35 MHz)	Zu gleichen Teilen zwei Satellitenbetreiber (XM, Sirius) und ein terrestrischer Betreiber
RUS, JAP:	2520-2670 MHz (150 MHz)	Dieses Band wird in Europa zukünftig dem Mobilfunk zugewiesen werden
EU:	1452-1492 MHz (40 MHz)	Unterhalb 1467,5 MHz terrestrischer-, oberhalb Satellitenbroadcast.

Daneben wird digitaler Hörrundfunk – mit unterschiedlichen Standards – über Fernmeldesatelliten im Ku-Band abgestrahlt (EUTELSAT und ASTRA).

Für den Empfang benötigt man ASTRA-ähnliche oder noch kleinere Antennen. Für den Empfang von *Digital Audio Broadcast* (DAB) genügt auch eine Stabantenne. Das terrestrische DAB ist in Deutschland zögerlich angelaufen. Die Firma *WorldSpace* realisierte einen Satelliten-DAB-Dienst für die Karibik, Afrika, Europa, Indien und den Pazifik, der auch in Deutschland empfangbar ist.

Diese Satelliten arbeiten im Band 1452–1492 MHz. In den USA werden seit 2000 zwei *Digital Audio Radio Systems* (DARS; XM und Sirius) bei 2,3 GHz betrieben. Für ihren Empfang genügen sehr kleine Antennen am Fahrzeug.

In Japan ist das ESS Satelliten-DARS geplant. ESS, XM, Sirius und WorldSpace senden im MP3-Standard, in dem auch das Internet Tausende von Audio-Titeln ausstrahlt. MP3 ist im Wesentlichen das Audio von MPEG-2/Layer-3 (siehe Videokomprimierung, Kap. 4.2.3).

Das terrestrische DAB wird in Europa nach dem Standard EUREKA-147 abgestrahlt, der 1986 definiert wurde. Inzwischen ist die Komprimierung weiter fortgeschritten und ausserdem war EU-147 nicht für Satelliten geeignet. Es hat keinen nennenswerten *Interleaver*, das verwendete COFDM verursacht 2 dB Verlust im Satellitensender, die inkohärente Demodulation benötigt 3 dB mehr Leistung als QPSK (siehe Modulationsverfahren), der fehlende Reed-Solomon Code vergibt 4 dB Leistung (siehe Kanalcodierung), und die veraltete Komprimierung benötigt die doppelte Bitrate gegenüber MP3, also 3 dB mehr Leistung (siehe Digitale Übertragung), in der Summe ein Nachteil von 12 dB. EU-147 verhält sich zu MP3 wie D2MAC zu MPEG. Das EU-147 heute für ein zukünftiges DAB vorzusehen wäre, als wenn man einen *SuperPC* für den Markt von 2010 entwirft auf der Basis eines 286 Prozessors.

Die digitale Kurzwelle

Audioprogramme wurden in Europa ca. 1998 im Programm *Digital Radio Mondiale* (DRM) digital komprimiert. Für die weltumspannende Abstrahlung (in der Mittelwelle bei 526,5 bis 1606,5 kHz, in der Kurzwelle bei 25 670,0 bis 26 100,0 kHz etc.) verwendet man 16QAM und 64QAM, letzteres im Regelfall und das robustere 16QAM mit reduzierter Qualität in der Wiedergabe bei atmosphärischen und insbesondere ionosphärischen Störungen; der Sender schaltet störungsabhängig von einem Modulationsverfahren auf das andere um, und das Radio „zieht mit“.

Die digitale Kurzwelle überträgt den Audiokanal mit 23 kb/s, einem Zehntel der Übertragungsrates des *Digital Audio Broadcast* (DAB) bei gleicher subjektiver Qualität im Auto. Der Kurzwellsender sendet weltweit (und kann auch im Wald empfangen werden), während das DAB bei 1,5 GHz einen Sender alle zwanzig Kilometer benötigt (und nicht in den Wald oder die Strassenzeile hinein sieht).

Die Übertragung erfolgt terrestrisch; das Signal reflektiert an der Ionosphäre und ist damit auch jenseits des Horizontes empfangbar – nach sechs Reflexionen auf der anderen Seite der Erde.

4.2.5 3-D-Fernsehen

Beim 3-D-Fernsehen wird dem Bild die räumliche Dimension, die Tiefe hinzugefügt. Wegen des technischen Aufwandes bei Aufnahme und Wiedergabe und der höheren Übertragungskosten ist es bis Anfang der 80er Jahre über Versuchsendungen nicht hinaus gekommen. Das älteste Verfahren ist das 1850 entwickelte Anaglyphenverfahren (*Anaglyphe* – ein reliefartiges Kunstwerk). Es kam in den 50er Jahren wieder auf, als 3-D-Filme eine kurze Blüte erlebten. Weltweit wurden bis ca. 1990 etwa 250 3-D-Filme hergestellt.

1982 wurde in den dritten Fernsehprogrammen in Deutschland unter anderem der Film „Wenn die Bilder plastisch werden“ ausgestrahlt, der mit einer rot-grünen Brille in 3-D gesehen werden konnte. Innerhalb weniger Wochen wurden mehrere hunderttausend Anaglyphenbrillen verkauft. In den USA begann die Produktion von 3-D-Videos auf Kassette.

Man unterscheidet das stereoskopische, das autostereoskopische und das holographische Verfahren.

Es gibt drei stereoskopische Verfahren. Beim ersten Verfahren wird das Bild mit zwei im Augenabstand versetzten und mit unterschiedlichen Filtern (rot-grün) versehenen Objektiven aufgenommen. Die Bilder werden übertragen und leicht gegeneinander verschoben auf dem Bildschirm abgebildet. Die Brille (rechts rot, links grün) ordnet die Bilder dem Auge zu, so dass in der Verschmelzung der Bilder ein räumlicher Eindruck entsteht.

Beim zweiten Verfahren werden bei der Aufnahme mit einem Spiegel, der nur Rot und Grün durchlässt, die Rechts- und Linksbilder erzeugt. Diese werden übertragen, auf dem Bildschirm sichtbar gemacht und mit der rot-grünen Stereobrille den Augen zugeordnet.

Beim dritten Verfahren werden abwechselnd die Teilbilder der linken und rechten Kamera übermittelt; man schaut mit einer ungefärbten Brille mit einem elektronisch gesteuerten, mit dem Bildwechsel synchronisierten Verschluss, wobei den Augen im entsprechenden Rhythmus das Teilbild so zugeordnet wird, dass in der Verschmelzung der räumliche Eindruck entsteht.

Beim autostereoskopischen Verfahren wird die räumliche Bildwirkung mit einem speziellen (Flüssigkristall-)Bildschirm erzeugt, es wird keine Brille benötigt.

Die holographische Aufnahme (hologramm = ganz, unversehrt) des gesamten Bildes eines Objektes erlaubt seine Betrachtung von allen Seiten; es ist das aufwendigste Verfahren mit dem höchsten Aufnahme-, Übertragungs- und Wiedergabeaufwand.

Stand der Technik sind heute stereoskopische Verfahren in vielen Anwendungen in der Produktion bis hin zur Medizintechnik und insbesondere der Tele-Medizin und Tele-Chirurgie.

4.3 Verschlüsselung

Professioneller Datenschutz bei der Übermittlung ist für Industrie und Handel unabdingbar. Konkurrenzunternehmen und „befreundete“ Staaten in Ost und West

setzen immer umfangreichere Methoden der Industriespionage ein. Spätestens seit der Wiedervereinigung tobte dieser Wirtschaftskrieg, angeführt von USA, Russland und Frankreich.

Die USA spionieren in Deutschland unter anderem im Rahmen des 1947 begründeten Programms ECHELON (der Siegermächte USA, UK, Australien und Neuseeland). Der volkswirtschaftliche Schaden durch ECHELON in Deutschland beträgt ca. 1 Milliarde € pro Jahr.

Deshalb müssen Satellitenlinks, wie alle Funkstrecken und auch Kabel, geschützt werden, da alle Sendungen von jedem abgehört werden können, der eine entsprechende Anlage betreibt. Der Vorteil der Satellitenkommunikation *vis à vis* Richtfunk und Kabel ist, dass der Chryptographie hier eher Aufmerksamkeit geschenkt wird. In Wahrheit ist Richtfunk und Kabel einfacher abhörbar (mit Dipolantennen in der Verlängerung der Richtfunkstrecke) als der Satellitenfunk (mit einer Erdfunkstelle mit einigen Metern Durchmesser). Bei festen Leitungen gibt es Wege, im Schacht an das Kabel anzukoppeln – und hier ist die Glasfaser leichter abhörbar, als das Kupferkoaxialkabel.

Spezielle Codes und Schutzverfahren sind eine seit Jahrtausenden geübte Kunst, die durch den Einsatz elektromechanischer und dann elektronischer Geräte eine hohe Reife erreicht hat. Trotzdem werden auch solche Systeme immer wieder durchbrochen, wobei häufig menschliches Versagen (Fehler in der Handhabung) dem Codebrecher wertvolle Hinweise geben.

Die klassische Cryptographie wurde von den Diplomaten und Militärs verwendet. Die wohl älteste Anwendung dürfte der Grabstein von Menet Khufu in Ägypten 1900 v.C. sein; hier wurde dem Verstorbenen mit verschlüsselten Hieroglyphen eine Botschaft mit auf den Weg gegeben, die bis heute nicht entziffert wurde.

Alle anderen Chiffres wurden früher oder später geknackt. Am 17. Jan. 1917 entschlüsselten die Engländer das „Zimmermann Telegramm“, das von Berlin an die deutsche Botschaft in Washington gerichtet war und den Plan enthielt, Texas, Arizona und Kalifornien nach dem gewonnenen Krieg an Mexiko zu geben. Daraufhin erklärten die USA Deutschland den Krieg.

Am 07. Dez. 1941 entzifferte die amerikanische Marine den Inhalt eines Telegramms von Tokyo an die japanische Botschaft in Washington, das das Ende der diplomatischen Beziehungen zu den USA für 13:00 h (8:00 h in Hawaii) ankündigte. Die Regierung versäumte jedoch zu reagieren und verlor in Pearl Harbor in wenigen Minuten 2 403 Soldaten und acht Schlachtschiffe.

4.3.1 Verschlüsselungsprotokollebene

Versucht man die Nachrichtenverschlüsselung in die Protokollhierarchie des OSI-Modells einzugliedern, so erscheint zunächst die Ebene 6 (Präsentation; s. Abb. 8.12) logisch sinnvoll. Im Prinzip kann auf jeder Ebene verschlüsselt werden, insbesondere auch auf der physikalischen. Die Link-Ebene bietet hier Vorteile, wie z.B. die Verkehrsflussanalyse (*Traffic Flow Analysis*, wer spricht mit wem?), und das Einsetzen einer (verschlüsselten) Nachricht in einen permanenten Blindverkehr, so dass für den Gegner nicht erkennbar ist, ob eine Nachricht vorliegt.

Auf der anderen Seite steht das Interesse von Sender und Empfänger, die nur an „End-to-End-Verschlüsselung“ interessiert sind. Theoretisch könnte die Information vom Betreiber der Übertragungswege verschlüsselt werden, ohne den Endverbraucher damit zu belästigen. Dies wird in der Praxis weniger gemacht, da (1) die Zurechnerstrecke zum Endverbraucher – insbesondere wenn sie terrestrisch verläuft – ebenfalls schutzbedürftig ist, und (2) der Endverbraucher im Allgemeinen seine Information nicht dem Netzbetreiber anvertraut, sondern sie *End-to-End* selbst schützt und seine Schlüssel selbst verwaltet.

Bei den traditionellen Fernmeldeeinrichtungen ist dieser Unterschied oft schwer auszumachen; anders liegen die Dinge bei der paketorientierten Datenübertragung und ihrer Speichervermittlung (*store and forward*; speichern und weiterleiten).

Da wesentliche Steuerinformationen im *Packet Header* enthalten sind, muss dieser, wo er interpretiert wird, im Klartext vorliegen. Es ist aber nicht nötig, dass an diesen Stellen auch der Datenteil im Klartext vorliegt; es spricht vieles dafür, die schützenswerten Daten in der Ebene 7 (*Applikation*) oder 6 (*Präsentation*) für eine „End-to-End-Übertragung“ zu verschlüsseln und unabhängig davon auf der physikalischen Ebene nochmals für die jeweilige Strecke zu verschlüsseln, um dabei auch die *Header-Information* für einen potentiellen Lauscher uninterpretierbar zu machen. Es ist plausibel, dass diese beiden Verschlüsselungsarten verschiedene Cryptoverfahren verwenden.

Für den Funkkanal gibt es Verfahren der Verschleiierung, wie zum Beispiel die Bandspreizung (*Spread Spectrum*), bei der das Signal im Rauschen versteckt wird. *Spread Spectrum* ist jedoch keine Verschlüsselung (kein Cryptoverfahren).

4.3.2 Cryptoverfahren

Massgebend ist, dass der Algorithmus durch einen Schlüssel parametrisiert ist, der schnell austauschbar, aber sehr schwer zu brechen ist. Man geht davon aus, dass der Algorithmus dem potentiellen Lauscher bekannt ist, und dass nur der Schlüssel geheim ist. Die Verschlüsselungsverfahren werden unterteilt in die so genannten

- Substitutionsverfahren (*Substitutions Chiffres*) und
- Transformationsverfahren (*Transpositions Chiffres*).

Bei einem Substitutionsverschlüsselungsverfahren wird jedem Buchstaben beziehungsweise jeder Buchstabengruppe aus dem Klartext ein Buchstabe beziehungsweise eine Gruppe zugeordnet. Obwohl theoretisch selbst einfache monoalphabetische Verschlüsselung einen extrem hohen Schutz bietet (zum Beispiel $26! = 4 \cdot 10^{26}$ mögliche Schlüssel) kann ein solcher Code durch Enumerierung geknackt werden – speziell mit den heute verfügbaren Rechnern.

Wesentlich grössere Sicherheit als die monoalphabetische Substitution bieten polyalphabetische Verfahren wie zum Beispiel der *Vigenere Code*. Aber auch dieser hält einem beharrlichen Angriff nicht stand. Eine grosse Sicherheit bietet die individuelle Wurmverschlüsselung, wobei der Schlüssel nur einmal verwendet wird (*One Time Pad*); dieses Verfahren ist sicher gegen den gezielten Angriff, zu Kosten der Schlüsselverwaltung.

Die deutsche Wehrmacht hat im 2. Weltkrieg Schlüsselgeräte eingesetzt, die auf einem polyalphabetischen Substitutionsverfahren mit extrem hoher Periodizität des Schlüssels beruhten, die ENIGMA der Marine. Massgebend für die Wahl der ENIGMA war unter anderem, dass im Bewegungskrieg und bei der Vermittlung von Meldungen in Gebieten schlechter Infrastruktur nur Funkverkehr möglich war. Die grosse Anzahl an täglich zu übertragenden Meldungen machte den Einsatz eines automatischen Gerätes erforderlich.

Die deutschen Systeme wurden von den Alliierten geknackt, wobei Bedienungsfehler oder allzu wörtliches Festhalten an Dienstvorschriften den Cryptoanalytikern (auch in den USA) wertvolle Hinweise lieferten. Dazu kam ein nicht gerechtfertigtes Vertrauen in ENIGMA, obwohl von der Truppe starke Zweifel an seiner Sicherheit vorlagen.

Fünfundzig Jahre später kam ein Vorschlag der USA, alle Länder der Erde sollten ihre Schlüssel in einer Datei (*Clipper Chip*) in den USA ablegen. Bislang ist diesem Vorschlag niemand gefolgt.

4.3.3 Kategorien von Schlüssel und Codes

In den verschiedenen Möglichkeiten der Kategorisierung der Chiffrierverfahren können die Schlüssel für Ver- und Entschlüsselung folgendermassen sein:

- i identisch; für Ver- und Entschlüsselung wird derselbe Schlüssel verwendet
- ii invers; das Produkt von Ver- und Entschlüsselungsschlüssel ist gleich 1
- iii verschieden; keine der obigen Eigenschaften trifft zu.

Chiffrierverfahren, die denselben Schlüssel für Ver- und Entschlüsselung verwenden, nennt man symmetrisch, alle anderen asymmetrisch.

Die beiden am meisten verbreiteten Chiffrierverfahren sind der DES und das RSA. Der (symmetrische) DES macht die vorherige Verteilung des gemeinsamen (geheimen) Schlüssels notwendig, während das (asymmetrische) RSA ohne Verteilung des geheimen Schlüssels auskommt. Eine andere Kategorisierung ist in

- *Block Codes* (analog den *Block-Codes* für Fehlerschutz) und
- *Stream Codes* (analog den sequentiellen Codes - Viterbi-Code).

4.3.4 Der Data Encryption Standard DES

Der DES Algorithmus wurde 1976 von IBM (New York) entwickelt und von der NSA der USA modifiziert; er ist ein konventioneller Substitutionschiffre (Verwürfelungsalgorithmus) mit 16 aufeinander folgenden Substitutionen; die Sicherheit eines Substitutionschiffre wächst exponentiell mit der Anzahl der aufeinander folgenden Stufen.

Der DES-Schlüssel ist 56 bit lang und symmetrisch (derselbe Schlüssel wird für Ver- und Entschlüsselung verwendet), und muss vor der Übertragung zwischen Sender und Empfänger ausgetauscht werden.

Mit dem DES alleine ist keine „Digitale Unterschrift“ - und damit keine authentische Kommunikation - möglich.

Der DES ist heute der am meisten verwendete Chiffre für die laufende Übertragung (nicht für den Verbindungsaufbau); er wird auch bei Abonnementfernsehen (*Pay TV*) zur Verschlüsselung des TV-Bildes eingesetzt.

4.3.5 Das RSA Chiffrierverfahren

Ein lang gehegter Wunsch in der Verschlüsselung war es, keine Schlüssel austauschen zu müssen. Der Schlüssel des Partners sollte im Telefonbuch stehen. Die Chiffrierer Ronalt Rivest, Adi Shamir und Leonard Adleman am *Massachusetts Institute of Technology (MIT)* wurden 1977 aufgefordert, zu beweisen, dass dies nicht möglich ist. Stattdessen entwickelten sie ein Transformationsverfahren, einen Falltür-Agorythmus (*Trap Door Cipher*), der einfach in eine Richtung gebildet und vergleichsweise schwierig zu reversieren ist und so die Veröffentlichung des Schlüssels im Telefonbuch ermöglicht.

Ein sehr versimpliziertes Beispiel ist die Exponierung mit 237; nur mit Bleistift und Papier und Geduld kann man eine 17-stellige Zahl 237 mal mit sich selbst multiplizieren; mit Bleistift und Papier allein zieht man aber nicht einfach die 237-te Wurzel aus einer 4029-stelligen Zahl.

Allgemein: Es ist einfach, für $y = f(x)$ die Form $x = f^{-1}(y)$ zu bilden, wohingegen es höchst aufwendig ist, von $x = f^{-1}(y)$ zu y zurück zu finden.

Trotz Kenntnis des öffentlichen Schlüssels e ist es nicht möglich, auf den geheimen Schlüssel $d = e^{-1} \{ \text{mod}[(p-1)(q-1)] \}$ zu schliessen, da hierzu eine Faktorisierung (Primfaktorzerlegung) von $n = p \cdot q$ beziehungsweise $(p-1) \cdot (q-1)$ nötig ist:

► Der Codebrecher muss die bekannte Zahl n in die beiden sehr grossen Primzahlen p und q faktorisieren.

Dies ist für sehr grosse Primzahlen n ein zeitaufwendiges Verfahren. Die Rechenzeit steigt mit der Länge von n . Der Anwender muss einfach den Schlüssel in kürzerer Zeit wechseln, als *state of the art computing* für dessen Knacken beansprucht.

Wie funktioniert es?

Im Gegensatz zum DES ist das RSA-Verfahren ein Blockcode, und es ist asymmetrisch, das heisst, für den Schlüssel e , mit dem verschlüsselt wird, und dem geheimen Schlüssel d für die Entschlüsselung, gilt:

$$d \cdot e = 1 \text{ mod } [(p-1) \cdot (q-1)] \quad \text{bzw.} \quad d = e^{-1} \{ \text{mod } n \}. \quad (4.8)$$

wobei $\text{mod} = \text{„modulo“}$ und die Ziffern p und q vom Sender vor der Übertragung „zufällig“ gewählt (mindestens 100-stellige Primzahlen sind). Die zu übertragende Information M wird in eine ganze Zahl zwischen 0 und $n-1$ transponiert, so dass:

$$n = p \cdot q \quad (4.9)$$

Bei numerischen Daten dienen die Ziffern als Zahlen; Zeichendaten können Einzelziffern zugeordnet werden. Buchstaben können zum Beispiel durch ihre Positionsziffern im Alphabet wiedergegeben werden ($A = 01 \dots Z = 26$). Die Information »Aerospace« führt so zu „01 05 18 15 19 16 01 03 05“. Die Zahl n bestimmt die Grösse des einzelnen Übertragungsblocks. Die Verschlüsselung der Information M mit e und n in den Chiffre C erfolgt nach der Vorschrift

$$C = M^e \pmod{n}. \quad (4.10a)$$

Entsprechend erfolgt die Dechiffrierung mit dem geheimen Schlüssel, die ganze, positive Zahl d :

$$M = C^d \pmod{n}. \quad (4.10b)$$

Für den geheimen Schlüssel d gilt die Forderung ($\text{GGT} = \text{grösster, gemeinsamer Teiler}$)

$$\text{GGT}(d, [(p-1) \cdot (q-1)]) = 1 \quad (4.11)$$

falls sich $d, p-1$ oder $q-1$ faktorisieren lassen, gibt es keine gemeinsamen Faktoren.

Der Schlüssel d ist typischerweise 512 Bit (64 Byte) lang, kann aber linear verlängert werden, wodurch sich die Sicherheit exponentiell erhöht. Für seine numerische Bestimmung wird ein leistungsfähiger GGT-Algorithmus (*extended greatest common denominator algorithm*) verwendet. Der Sender bestimmt ausserdem den öffentlichen Schlüssel e und publiziert ihn in einer Art Telefonbuch.

Wie läuft es ab?

- (1) Der Sender A entnimmt B's öffentlichen Schlüssel e aus dem Telefonbuch, chiffriert damit die *Message* M zu M^e und sendet sie an B;
- (2) B empfängt die chiffrierte *Message*, wendet seinen geheimen Schlüssel d an und erhält damit $M^{e \cdot d} = M^1 = M$;
- (3) Jeder andere, der nicht über B's geheimen Schlüssel d verfügt, kann die verwürfelte *Message* nicht entschlüsseln;
- (4) Für die geschützte Transaktion muss kein Schlüssel ausgetauscht werden.

4.3.6 Elektronische Unterschrift

Verschlüsselt A die Nachricht M an B mit seinem geheimen RSA-Schlüssel d_A , so nennt man dies die digitale Unterschrift. Die Nachricht ist von A unterzeichnet.

4.3.7 Digitale Unterschrift

Verschlüsselt A die Nachricht M an B zuerst mit seinem geheimen Schlüssel d_A und zusätzlich mit dem öffentlichen Schlüssel e_B , wird B die empfangene *Message* zuerst mit seinem geheimen Schlüssel d_B entwürfeln. Im *Header* der *Message* wird ihm gesagt, die Nachricht komme (verschlüsselt) von A.

B nimmt den öffentlichen Schlüssel e_A aus dem Verzeichnis und wendet ihn auf die Nachricht an, um so den Klartext $M^{d^{e_A}} = M$ zu gewinnen.

Auf diese Weise ist nicht nur die Übertragung durch die zusätzliche Verschlüsselung erhöht geschützt, sondern insbesondere auch für B der Beweis erbracht, dass die Nachricht von A ist: Senderidentitätsbeweis (*Proof of Origin; Message Authentication*); nur A hat den geheimen Schlüssel d_A , mit dem er die Nachricht verschlüsseln konnte.

Neben der Authentisierung der Übertragung wird die Digitale Unterschrift auch zur Sicherung von Akten und abgelegten Dateien verwendet. Setzt man seine Digitale Unterschrift auf einen Datensatz, der abgelegt wird, kann zu einem späteren Zeitpunkt durch Entschlüsselung festgestellt werden, dass der Datensatz nicht verändert wurde.

Im Kerberos-System werden hierzu umfangreiche Dokumente nicht in Gänze »unterschrieben«, sondern in gezielten Auszügen – die ist die *Hash-Function*. Kerberos ist ein Produkt des MIT für die Digitale Unterschrift und Dokumentensicherung; vom MIT stammt auch das RSA.

4.3.8 Steganographie

Neben dem Verschlüsseln (Chryptographie, dem Verschleiern von Daten) steht das Verstecken von Daten (Steganographie). Dies geht auf das i-Tüpfchen der Deutschen Wehrmacht zurück, das eine vielfach verkleinerte Textseite war und in einem Routinedokument unerkannt verschickt wurde. Heute verwendet man Rechnerdateien (U-Boote), Audio und Video für Steganographie.

Durch Modulation des Least Significant Bit eines Audiosignals kann, über Zeit, beliebig viel Information übermittelt werden, ohne Veränderung des Signals, und das menschliche Ohr hört den Unterschied nicht.

Im Video moduliert man das *Least Significant Bit* der Helligkeitskomponente. Bei 256 Helligkeitsstufen, also 8 Bit für die Helligkeit, plus je 8 Bit für Rot/Grün/Blau kann auch im Video beliebig viel Information, für das menschliche Auge unsichtbar, versteckt werden. Gängige Steganographie-Programme sind Steganos, Hide & Seek, StegoDos etc.

4.3.9 Schlüsselgebrauchsdauer und Schlüsselaustausch

Die Lebensdauer eines Schlüssels darf die für sein Knacken (mit modernsten Rechnern) notwendige Zeitdauer nicht übersteigen. Da die rechnergestützte Generierung von Schlüsseln beliebig einfach ist, sollten Schlüssel sinnvoll frequent erneuert werden.

Der höchstmögliche Schutz wird dann erreicht, wenn der Schlüssel nach jeder Übertragung ausgewechselt wird. Diese Einmalverwendung (*One Time Pad*) ist das Antipodal zur monatelangen Verwendung desselben Schlüssels.

Der Schlüsselaustausch zwischen den Partnern einer Verbindung muss geschützt erfolgen, um die nachfolgende Übertragung nicht zu gefährden; sie sollte deshalb, wenn möglich, nicht über die Strecke getätigt werden, über die dann die

Übertragung abgewickelt wird. Wenn kein sicherer Kanal zur Verfügung steht, gibt es Verfahren, die dennoch den sicheren Austausch der Schlüssel ermöglichen – wie zum Beispiel das in Abb. 4.6 skizzierte:

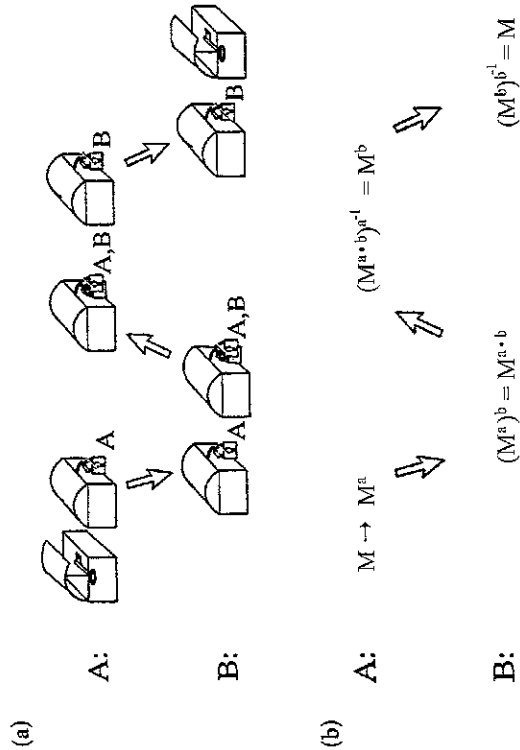


Abb. 4.6 (a) Der sichere Schlüsselaustausch über unsichere Kanäle (ikonische Darstellung), (b) der sichere Schlüsselaustausch über unsichere Kanäle (algebraische Form)

- (1) A legt seinen Schlüssel „A“ in die Truhe, sperrt sie mit seinem Schlüssel „A“ zu und schickt sie an B,
- (2) B kann die Truhe nicht öffnen; was ihm bleibt, ist die Truhe mit seinem Schlüssel „B“ zusätzlich zu verschliessen und sie an A zurück zu senden,
- (3) Nun kann A sein Schloss „A“ abnehmen und die Truhe – immer noch mit dem Schloss „B“ verschlossen – sicher an B schicken,
- (4) Nach Erhalt, wird nun B sein Schloss mit seinem Schlüssel „B“ entfernen, die Truhe öffnen, den Schlüssel „A“ entnehmen und an A verschlüsselte Informationen senden.

Das Diffie-Hellman-Key Exchange

Das von W. Diffie und M. Hellman 1976 entwickelte Verfahren zur Erzeugung eines gemeinsamen Schlüssels funktioniert wie folgt:

Man bestimmt eine grosse Primzahl p mit > 100 Dezimalstellen, also von der Größenordnung 10^{100} beziehungsweise 2^{332} (mit z.B. 256 bit) und eine teilerfremde Zahl $s > p$. Weiterhin wählen A die Zufallszahlen $a < p$ und B die $b < p$. Dann,

A: $\alpha = s^a \pmod{p}$ und sendet es an B	B: $\beta = s^b \pmod{p}$ und schickt es an A
$K = \beta^a \pmod{p} = s^{a \cdot b} \pmod{p}$	$K = \alpha^b \pmod{p} = s^{a \cdot b} \pmod{p}$

Die Partner haben den gemeinsamen Schlüssel K bestimmt. Die geheimen Zahlen a und b wurden nicht der Übertragung ausgesetzt – nur α und β . So lange A und B ihre Geheimzahlen a und b nach der Ermittlung von K unwiederbringbar löschen, muss nur noch der gemeinsame, symmetrische Schlüssel K sicher gehandhabt werden.

Der Schutz des *Diffie-Hellman Key Exchange* beruht auf der numerischen Schwierigkeit, diskrete Logarithmen in endlichen Primkörpern zu berechnen, aus α oder β die Zufallszahlen a und b zu berechnen, und daraus dann den Schlüssel K . Der Codebrecher muss sowohl den diskreten Logarithmus p finden, um mit $s^p = a \pmod{p}$ die Geheimzahl a zu bestimmen, und durch den diskreten Logarithmus y für die Bestimmung von b , um $K = s^{a \cdot b} \pmod{p}$ zu berechnen.

4.3.10 Verschlüsselung im Mobilfunk

Der GSM-Mobilfunk, wie auch GlobalStar, sind Beispiele für die Verschlüsselung mit RSA. Diese Netze benutzen einen Teilnehmerschlüssel „Ki“ (*Key individual*), der auf dem Mikrochip der *Subscriber Identity Module* (SIM Karte) des D-Handys „eingebrennt“ ist, also nie wieder aus der Karte ausgelesen werden kann, ohne sie zu zerstören. Dieser *Secret Key* ist 128 Bit lang (eine 40-stellige Dezimalzahl) und schützt vor Gebührensmissbrauch durch Hacker.

Wählt der Teilnehmer an, prüft die Netzwerkkontrolle seine Identität durch Übersendung einer beliebigen Kennungsnachricht zum Handy beziehungsweise zur SIM-Karte, die willkürlich generierte Zufallszahl RAND (ebenfalls 128 bit lang), die mit dem öffentlichen Schlüssel des durch die Rufnummer identifizierten Teilnehmers chiffriert ist.

Das Handy dechiffriert die Kennungsnachricht „GRES“ mit seinem geheimen Schlüssel (und dem RSA A3/A8-Algorithmus) und sendet die entschlüsselte Kennungsnachricht zur Netzkontrolle zurück. Stimmt sie, wird der Sprechkreis freigegeben. Die Kennungsnachricht ist bei jeder Gesprächsanmeldung eine andere, so dass das Mithören dieses Vorganges keine verwertbaren Erkenntnisse für den Hacker bringt.

Selbst der öffentliche Schlüssel des Teilnehmers wird von den Netzbetreibern geheim gehalten. Die beiden sicherheitsrelevanten Daten, der geheime und der öffentliche Schlüssel, werden zu keiner Zeit über das Netz übertragen. Den „Ki“ zu knacken bedeutet, eine 128 bit lange Binärzahl aus $3,4 \cdot 10^{38}$ möglichen Kombinationen zu finden.

Diese Sicherheit besteht jedoch nur auf der Strecke von und zum GSM-Funknetz (bzw.) GlobalStar-Gateway. Von dort wird das Gespräch unverschlüsselt im öffentlichen Wählnetz zum Ziel geleitet und kann auf dem Weg dorthin abgehört werden. Es gibt aber auch GSM-Handys, die *End-to-End* verschlüsseln. Nach Aufbau der Verbindung wird auf Knopfdruck die zusätzliche Verschlüsselung aktiviert.

4.3.11 Gesetzliche Überwachung

Gerade in demokratischen Ländern darf der Staat (die Staatsanwaltschaft) unter definierten Voraussetzungen den Post- und Fernmeldeverkehr mit expliziter gerichtlicher Verfügung einsehen (*Legal Interception*). In der Deutschland ist dies

Tabelle 4.3 Faktoren, Themen und Aspekte der geschützten Übertragung

Faktor	Thema	Inhalt
Nutzer	<i>Authentication</i>	Der Beweis, dass die Nachricht von einer identifizierten und authentifizierten Person kommt (<i>Proof of Origin</i>)
	<i>Authorization</i>	Autorisierung der Dienstenutzung eines Netzes: Kein unautorisiertes Absenden von Daten – selbst von autorisierten Personen
	<i>Certification</i>	der Nutzer und der Schlüssel werden von einer Betreiberorganisation zertifiziert
Nachricht	<i>Integrity</i>	Unversehrtheit der Nachricht: Keine Korruption der Daten
	<i>Privacy</i>	Verschwiegenheit: die Vertraulichkeit des Inhaltes der Nachricht muss gegen Abhören bewahrt werden
	<i>Non-Repudiation</i>	Nicht-Leugnung: Der Beweis für den Sender, dass der Empfänger die Nachricht erhalten hat
Übertragung	<i>Confirmation</i>	Empfangsbestätigung vom Empfänger, so dass keine Wiederholendung passieren kann – unabsichtlich oder böswillig
	<i>Traceability</i>	Verfolgbarkeit und Nachverfolgbarkeit der Übertragung
	<i>Auditability</i>	Überwach- und Buchhaltbarkeit der Übertragung
Netz	<i>Service Availability</i>	Verfügbarkeit des Kommunikationsdienstes
	<i>Security</i>	Sicherheit des Kommunikationsdienstes; keine Störung im Netz

im Gesetz zu Artikel 10 des Grundgesetzes, dem so genannten „G-10 Gesetz“, verankert. Der RSA-Algorithmus schien am Anfang – im Gegensatz zum DES – zu sicher, drohte Strafverfolgern dieses Instrument aus der Hand zu nehmen. Durch den Lizenzierungszwang wird sichergestellt, dass die RSA-Sicherheit nur im legalen Umfeld Einsatz findet.

4.3.12 Zusammenfassung zur Verschlüsselung

Die Verschlüsselung der Kommunikation im zivilen wie im militärischen Umfeld, in der Geschäftswelt wie im privaten Bereich, ist sinnvoll und notwendig. Schlüssel können umso leichter geknackt werden, je mehr verschlüsselter Text verfügbar ist (je länger der Schlüssel im Gebrauch bleibt), je mehr Information über den Klartext bekannt ist (Galileo-Positionsinformation zu verschlüsseln wäre von begrenzter Nützlichkeit, da der Klartext, die Koordinaten, mit alternativen Sys-

temen in Erfahrung gebracht werden können) und je leistungsfähiger der Rechner des Knackers ist.

Der letzte Punkt macht es von Jahr zu Jahr mit der fortschreitenden Leistungsfähigkeit auch kleiner Rechner schwerer, Information zu schützen. Ein Verschlüsselungsverfahren, das heute noch als sicher gilt, kann in ein bis zwei Jahren schon mit einem gängigen *Notebook* geknackt werden.

Man ist gezwungen, die Verschlüsselungsverfahren ständig fortzuschreiben. Das Problem dabei ist nicht die Konstruktion besser Verschlüsselungsverfahren, sondern deren Installation bei den Nutzern und die Akzeptanz der Nutzer, sich ständig neue Verfahren installieren zu lassen und zu verwenden. Ein Verschlüsselungsverfahren in einer Firma oder Firmengruppe ist nur nützlich, wenn alle Gegenstellen es eingerichtet haben und auch benutzen.

4.4 Multiplexing

Multiplexverfahren und Vielfachzugriff führen zu sehr ähnlichen Abkürzungen (z.B. FDM und FDMA), sind aber verschiedene Vorgänge. Beim Multiplexing sind die Signale (z.B. FDM) im Basisband gebündelt; beim Vielfachzugriff der einzelnen Teilnehmer (z.B. FDMA) werden die Hochfrequenzträger in der Frequenz gestaffelt (siehe Kap. 6). Sowohl Bündelung als auch Vielfachzugriff-Bündelung können in der Frequenz (F), in der Zeit (T) oder im Code (C) stattfinden.

4.4.1 Das Frequenzbündelungsverfahren FDM

Im *Frequency Division Multiplex* (FDM; auch *Frequency Division Duplex* (FDD)) werden Einzelsignale auf einen Basisbandträger gebündelt (*gemultiplext*), dieser moduliert und in die Hochfrequenz umgesetzt. Die Signale sind analog oder digital; ihre Modulation kann analog (zum Beispiel FM) oder digital (nach Analog/Digital-Wandlung) sein. FDM spielt jedoch vorwiegend in analogen Systemen (wie zum Beispiel bei INTELSAT und INTERSPUTNIK) eine dominierende Rolle, wird aber in neueren Systemen von TDM verdrängt.

FDM, COFDM, OFDMA, OFHMA

Im Allgemeinen (FDM bzw. *Coded Orthogonal Frequency Division Multiplex* (COFDM), *Orthogonal Frequency Division Multiple Access* (OFDMA) und *Orthogonal Frequency Hopping Multiple Access* (OFHMA)) werden digital modulierte Einzelträger (SCPC) so äquidistant OFDM frequenzgestaffelt, dass ihre Kanalseparation ihrer normalisierten Bitrate (BR) entspricht: 100 kHz Staffeln für 100 kbit/s Träger bei BPSK bzw. 50 kHz Staffeln für 100 kbit/s Träger bei QPSK; die Bandbreite ist:

$$BW = \frac{BR}{\lg_2(\text{Anzahl der Phasenzustände})}$$

(4.12)

Die Spektrumsnebenkeulen fallen in die Nullstellen des Frequenzspektrums (sie sind orthogonal zu ihnen). Hinzu kommt, dass die digitalen Träger störresistenter als analoge Träger sind. Orthogonale Polarisationen in benachbarten Frequenzen erhöhen den Störabstand.

Mit zum Beispiel der Rate $1/2$ Codierung und *Interleaving* kann die Bitfehler-rate reduziert werden. Bei COFDM wird zusätzlich das einzelne Signal über die Summe der Frequenzen hüpfen, damit Mehrwegeeffekte, die einzelne Frequenzen auslöschen können, gemindert werden – ein FDM/FH-Verfahren. Im Gegensatz zu herkömmlichem FDMA mit starren Trägerfrequenzen, hüpfen die einzelnen Träger – nach einem vorgegebenen Code, daher „*Coded...*“.

So wird zum Beispiel digitaler (Satelliten-) Hörrundfunk (DAB-EUREKA-147) abgestrahlt. Beim DECT, das in COFDM arbeitet, sind es 90 Frequenzen, über die das laufende Gespräch hüpfen und die jeweils beste aussucht. Bei DAB ist es 1,536 MHz bei 1,5 GHz, also 1‰ der Wellenlänge – nicht hinreichend, um Mehrwegeeffekte zu eliminieren; hierzu wären etwa 25% Versatz der Wellenlänge notwendig. Es werden zum Beispiel in 1,536 MHz 192 Träger benutzt, deren Abstand der Bitrate des Einzelträgers (12 kbit/s) entspricht (Orthogonalität). Die Gesamtbitrate ist $192 \cdot 12 = 2,3$ Mbit/s.

Der Vorteil des COFDM gegenüber einem in TDM gefassten Gesamt-Bitstrom ist, dass der Empfänger schmalbandig immer nur einen Träger ($1/192$ aller Programme) empfangen können muss. Allerdings muss er mikrosekunden-schnell durch das Spektrum hüpfen und einen Schmalbandträger nach dem anderen akquirieren.

Um die Demodulation des über die Frequenz hüpfenden Trägers zu erleichtern, wird differentielles QPSK (DQPSK; keine Trägersaufbereitung) eingesetzt.

Zur verbesserten Separierung aufeinander folgender Datenbündel lässt man einen zeitlichen Schutzabstand von 20%. Damit liegt die Spektrumsnutzungseffizienz bei 80%, und da beide Polarisationen belegt werden, sind es 40%.

Zur höheren Separierung benachbarter Kanäle sind sie in orthogonaler Polarisation. Damit wird die Effizienz der Spektrumsnutzung von 2 (bit/s)/Hz auf 1 (bit/s)/Hz reduziert, abzüglich des zeitlichen Schutzabstandes von 20% schließlich auf 0,8 (bit/s)/Hz.

Ein Vorteil ist die durch das *Frequency Hopping* (FH, im Verbund mit Interleaving und Codierung) erzielte Resistenz gegen Mehrwegeeffekte.

Der Nachteil von FDM liegt in der Intermodulation der Einzelträger. In der terrestrischen Anwendung lassen sich grosse *Backoffs* realisieren. In Satellitenanwendungen sind grosse *Backoffs* kostspielig.

Auch wird mit COFDM keine höhere Spektrumsnutzungseffizienz als mit gewöhnlichem QPSK erreicht (0,8 (bit/s)/Hz). Ob der Empfang eines kohärent durchlaufenden Bitstroms hoher Rate oder die rapide Folge von frequenzversetzten Einzelbündeln leichter zu realisieren ist, hängt vom Empfängerdesign und von den Stückzahlen ab.

OFDMA (Orthogonal Frequency Division Multiple Access), Vielfachzugriff nach dem *Coded-Orthogonal*-Verfahren, wird auch in WIMAX (*Worldwide Interoperability for Microwave Access*) eingesetzt, ein terrestrisches Funknetz nach dem IEEE

802.16 Standard. Dort wird mit 256 PSK moduliert, so dass 108 Mbit/s in 28 MHz übertragen werden können.

4.4.2 Das Zeitbündelungsverfahren TDM

Im Zeitmultiplex *Time Division Multiplex* (TDM; auch *Time Division Duplex* (TDD)) werden Einzelsignale in Zeitschlitzen auf einem Hochfrequenzträger angeordnet. TDM ist das Pendant zum TDMA-Verfahren, bei dem jedes Einzelsignal von einem anderen Sender kommt. TDM ist TDMA im Durchsatz überlegen, da die von nur einer Station auf den Träger modulierten Zeitsignale im Gegensatz zu TDMA keinen Schutzabstand zwischen aufeinander folgenden Zeitschlitzen benötigen.

So benötigt bei INMARSAT das *Outbound*-TDM eine Übertragungsrate von 1,2 kbit/s (für 22 Zeitschlitze à 50 bit/s) während das *Inbound*-TDMA 4,8 kbit/s einnimmt, also 25% Wirkungsgrad relativ zu TDM; hier lässt der Signallaufzeit-schutzabstand gleichzeitig Nutzer im Subsatellitenpunkt (35 780 km) und am Erdrand (41 680 km) zu; der Laufzeitunterschied beträgt 16,5% oder 20 ms.

TDM ist wesentlich einfacher zu empfangen als TDMA, bei dem der Rahmen in jedem Zeitschlitz neu akquiriert werden muss, in Frequenz, Phase, Bittakt und Rahmenformat.

Dies führt zu höheren Kosten beim Empfänger. Deshalb verwendet man in Netzen mit einer grossen Zahl von Empfängern, wenn immer möglich, TDM. Dies wird im Rundfunk von Ton- und Fernsehprogrammen so gemacht.

Wie kann der Satellit einzelne, von geographisch verstreuten Studios gesendete Programme in TDM abstrahlen? Man sendet sie im TDMA zum Satelliten und setzt sie an Bord um (*On Board Processing*; OBP), so dass sie im TDM abgestrahlt werden können.

4.4.3 Das Codebündelungsverfahren CDM

In Analogie zu TDM und FDM könnten Signale im *Code Division Multiplex* (CDM) im Basisband überlagert werden, das dann für die Übertragung moduliert würde. Hierzu müssten die Signale bandgespreizt werden – typischerweise um einen Faktor 10^3 bis 10^6 . Damit würde die benötigte Hochfrequenzbandbreite um 10^3 bis 10^6 grösser. Diesem Bandbreitenanspruch stünde jedoch kein Systemgewinn gegenüber.

Eine Ausnahme sind wohl die Navigationssignale bei GPS und Galileo, die zwei Codes (C/A und P bei GPS) im Basisband (in der Tonfrequenz) überlagern.

4.5 Kanalcodierung

Die Nützlichkeit der Codierung für Fehlerschutz ist bekannt. Gerade bei Satellitenstrecken mit ihrem sehr langen Weg durch die Atmosphäre ist Fehlerschutz sinnvoll. Daneben ist Datenschutz prinzipiell ratsam. Im Gegensatz zu Datenschutz fordert

Fehlerschutz zusätzliche Code-Bit, so dass aus n Nutz-Bit m Gesamt-Bit werden; die Code-Rate cr ist definiert als:

$$cr = \frac{n}{m}. \quad (4.13)$$

$$BER = \text{Anzahl der Nutzbit/Anzahl der Gesamtbit} \quad (4.14)$$

ist die Bitfehlerrate (*Bit Error Rate*). Im Mobilfunk und Geschäftsverkehr ist die Effizienz von Codierverfahren unterschiedlich: Beim Mobilkanal wird durch Codierung mit 33% zusätzlichen Bit eine Verbesserung von > 10 dB erreicht, bei $BER = 10^{-4}$ Bitfehlerrate (s. Abb. 4.8), was ohne Codierung nur mit um > 10 dB höherer Leistung erreicht würde.

Der für die jeweilige Anwendung zutreffende Code-Gewinn ist im Allgemeinen sehr von der Eingangsbitfehlerrate abhängig (s. Abb. 5.6); ein durchschnittlicher Code-Gewinn cg (CG in dB) als Funktion der Code-Rate $cr = n/m$ kann approximiert werden mit der Form

$$CG = 3 \text{ dB} - 10 \log(cr) \quad \text{für } cr < 1. \quad (4.15)$$

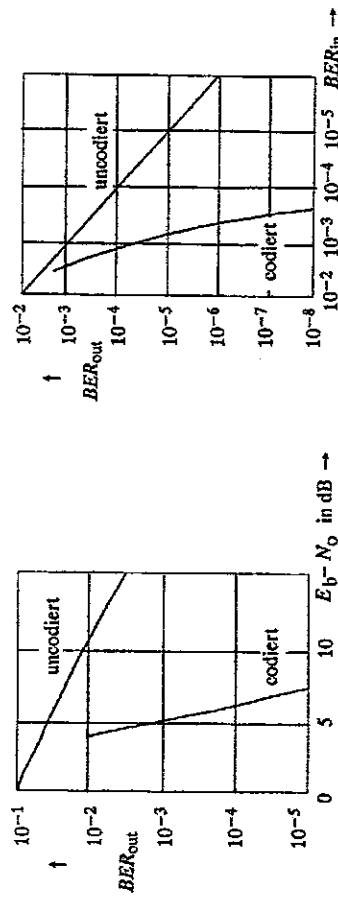


Abb. 4.7 Codierung im Mobilfunk mit 33% Code-debit

Abb. 4.8 Reed-Solomon-Codierung mit 4,7% Codebit

Der in Abb. 4.7 gezeigte *Convolutional Code/Viterbi* Decodierung bringt substantielle Verbesserung der Bitfehlerrate im Mobilfunk. Neuere Codes dieser Art in der *Vectorcoding*-Familie produzieren bis zu 10 dB Codiergewinn bei Rate $1/2$ und $BER = 10^{-12}$.

Abbildung 4.8 zeigt einen Reed-Solomon Block-Code mit $m = 255$, $n = 243$ für die Geschäftskommunikation. Er produziert mit nur 4,7% zusätzlichen Bit ($cr = 20/21$) eine Fehlerverbesserung von $3 \cdot 10^{-4}$ auf $1 \cdot 10^{-8}$, was ohne Codierung ≈ 4 dB mehr Sendeleistung erfordern würde.

Damit ergeben sich die folgenden Code-Gewinne als Funktion der Code-Rate cr , noch ohne *Vectorcoding*:

Tabelle 4.4 Typische Code-Gewinne (QPSK mit $BER = 10^{-5}$) gegen Code-Rate⁷

Code-Rate $cr = n/m$	1/1	15/16	7/8	5/6	3/4	2/3	1/2
Bitratenerhöhung ⁸	0,0 dB	0,3 dB	0,6 dB	0,8 dB	1,2 dB	1,8 dB	3,0 dB
Uncodiertes $E_b - N_0$	9,6 dB	9,6 dB	9,6 dB	9,6 dB	9,6 dB	9,6 dB	9,6 dB
Codiertes $E_b - N_0$	9,6 dB	6,3 dB	6,0 dB	5,8 dB	5,5 dB	4,8 dB	3,6 dB
Codegewinn CG	0,0 dB	3,3 dB	3,6 dB	3,8 dB	4,2 dB	4,8 dB	6,0 dB

Block Codes

Mit n Bit können nI Code-Wörter generiert werden (n Zeichen können in nI Permutationen angeordnet werden). Man benutzt aber nur eine Untermenge aller Code-Wörter, so dass sie sich in x Bit voneinander unterscheiden – die *Hamming-Distanz* zweier Code-Wörter. Fehlerhaft empfangene Wörter werden dem Code-Wort kleinster Hamming-Distanz zugeordnet. Wenn sich die Code-Wörter um nur ein Bit unterscheiden würden, würde der Fehler von einem Bit zur Fehlinterpretation eines anderen Code-Worts führen.

Wenn sich die Code-Wörter um zwei Bit unterscheiden, kann der Fehler von einem Bit festgestellt werden, aber nicht korrigiert werden, da die zwei benachbarten Code-Wörter wahrscheinlich gleich sind (gleiche *Hamming-Distanz* haben).

Mit drei Bit Unterschied zwischen den Code-Wörtern kann ein Fehler von einem Bit detektiert und korrigiert werden.

Ist zum Beispiel

das empfangene Code-Wort 01 00 01 1,

das nächstliegende Code-Wort 01 01 01 1, und

das entferntere Code-Wort 01 01 00 0, dann

wird der Decoder das nächstliegende Code-Wort wählen, weil es die kleinere *Hamming-Distanz* zum empfangenen Code-Wort als das entferntere Code-Wort aufweist. Man nimmt an, dass es wahrscheinlicher ist, dass ein Bit falsch war, als dass zwei Bit falsch waren.

Mit vier Bit Unterschied zwischen den Code-Wörtern kann ebenfalls ein Bit korrigiert und ein Fehler von zwei Bit detektiert werden. Zusammenfassend:

1 Bit Unterschied, 0 Fehl-Bit feststellen, 0 Fehl-Bit korrigieren

2 Bit Unterschied, 1 Fehl-Bit feststellen, 0 Fehl-Bit korrigieren

3 Bit Unterschied, 1 Fehl-Bit feststellen, 1 Fehl-Bit korrigieren

4 Bit Unterschied, 2 Fehl-Bit feststellen, 1 Fehl-Bit korrigieren

5 Bit Unterschied, 2 Fehl-Bit feststellen, 2 Fehl-Bit korrigieren

6 Bit Unterschied, 3 Fehl-Bit feststellen, 2 Fehl-Bit korrigieren usw.

Man wählt ein Codierverfahren mit einer ungeradzahigen Anzahl von n Bit, das dann $(n - 1)/2$ bit korrigieren kann, oder das nächst höhere Verfahren, das auch

⁷ nach EBU DT/III-C'93

⁸ und damit Erweiterung der benötigten Bandbreite

nur $(n-1)/2$ bit korrigieren, aber $n/2$ Fehl-Bit detektieren und an ein ARQ System zur nochmaligen Übertragung melden kann.

So werden bei der Block-Codierung die empfangenen Daten in einen Block (das Code-Wort) eingelesen und verarbeitet; das erste decodierte Bit erscheint nach einer Verzögerung entsprechend der Einlesedauer.

Sequentielle Codes, Convolutional Coding, Viterbi Decoding

Wie bei den Block-Codes der empfangene Block mit den zulässigen Code-Wörtern verglichen und dasjenige ausgewählt wird, das in den wenigsten Bits vom Empfangswort abweicht (es gibt eine endliche Zahl von zulässigen Code-Wörtern), hat das Zustandsgitterwerk (Treillis; s. Abb. 4.9) der sequentiellen Codierung (Convolutional Encoding) nur eine endliche Anzahl von zulässigen Pfaden; der Viterbi-Decoder ordnet die fehlerhaft empfangene Sequenz dem nächstliegenden, zulässigen (in der kleinsten Anzahl von Bit abweichenden) Pfad zu, sequentiell, Bit für Bit).

Der Faltungscodierung (Convolutional Encoding) prägt der Bitfolge also eine Signatur auf, eine endliche Anzahl von zulässigen Pfaden durch das Treillis (Zustandsgitterwerk). Im folgenden Fallbeispiel (s. Abb. 4.9) gibt es beispielsweise keine Pfade von Ebene 3 zu Ebene 1, von Ebene 3 zu Ebene 4 etc. Es sind immer nur zwei von vier Pfaden von jedem Zustand zum nächsten möglich.

Der Viterbi-Algorithmus korrigiert die fehlerhafte Empfangsbitfolge durch Wahrscheinlichkeitsmaximierung (Maximum Likelihood Decoding) und findet den Pfad durch das Treillis auf der Basis der kleinsten Anzahl von Fehlern (Minimum Distance Decoding). Da Maximum Likelihood und Minimum Distances für den binären symmetrischen Kanal identisch sind, kann der Convolutional Code (Faltungscodierung) durch den Pfad kleinster Abweichungen dargestellt werden.

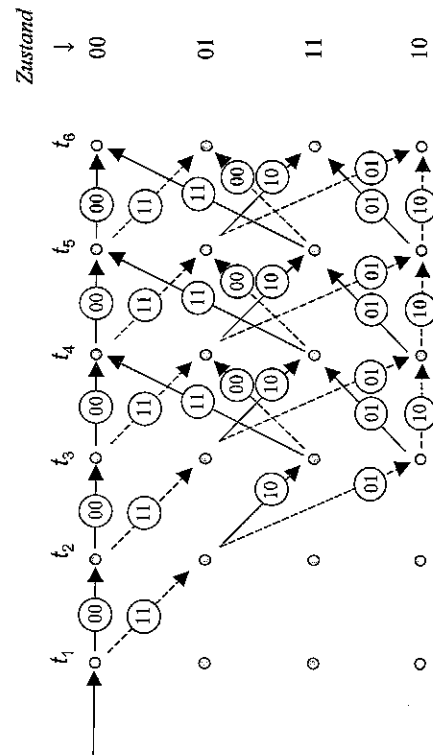


Abb. 4.9 Das Zustandsgitterwerk (Treillis) der sequentiellen Codierung

Bei der sequentiellen Codierung (Faltungscodierung) werden die Nutzbit mit Codebit gefaltet. Im Bild

sind die Daten 1 0 1 1 0
gefaltet zu 11 10 11 00 11;
empfangen wird 11 10 10 00 11.

Der Weg durch das Treillis führt zum Zeitpunkt t_2 zur Ebene 2 (e_2), dann zur Ebene 3 (e_3) zum Zeitpunkt t_3 , dann zurück zur Ebene 1 (e_1) zum Zeitpunkt t_4 , bleibt auf Ebene 1 (e_1) zum Zeitpunkt t_5 und schliesslich zur Ebene 2 (e_2) zum Zeitpunkt t_6 . Dieser Pfad beinhaltet, trotz des dritten Wegabschnitts nach Ebene 1 anstatt zur Ebene 2, nur einen Bit-Fehler, während die Alternative zum Zeitpunkt t_3 , zur Ebene 2 zu gehen, am Ende 3 Bit-Fehler beinhalten würde.

So wird die Entscheidung in t_4 erst nach Sichtung von t_6 getroffen; auch der sequentielle Code hat, ähnlich dem Block-Code, eine Verzögerung. Der Länge beim Block-Code entspricht die so genannte Verflechtungslänge (Constraint Length) beim Sequentiellen Code, die Anzahl der Symbole, die abgewartet werden, damit sie auf die aktuelle Zuordnung einwirken können, um die das Signal verzögert wird.

Kaskadierte Codierung

Es ist möglich, mehrere Codes in Serie anzuordnen und damit den Gesamcodegewinn zu erhöhen. Da zum Beispiel der Reed-Solomon-Code für grosse Bitfehlerarten kaum einen Gewinn erzielt (für die Eingangsbitfehler率 10^{-2} ist $BER_{out} = 10^{-2}$, keine Verbesserung; s. Abb. 4.9), für geringe Bitfehler率 jedoch enorme Gewinne liefert (bei $BER_{in} = 10^{-4}$ wird $BER_{out} = 10^{-11}$), codiert man Signale hoher Fehler率 zuerst mit einem robusten Viterbi Rate 1/2 Code, der das Signal auf zum Beispiel 10^{-4} anreichert und folgt mit einem „7/8 Reed-Solomon“-Blockcode.

Abbildung 4.10 zeigt die Konzeption von innerem und äusserem Code und Interleaver und Abb. 4.11 das prinzipielle Blockschaltbild. Die Bezeichnung *innerer Code* wird vom Übertragungskanal aus gesehen. Noch vor dem (inneren) „cr =

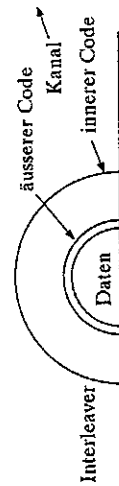


Abb. 4.10 Das Konzept Daten, innerer Code/äusserer Code/Interleaver

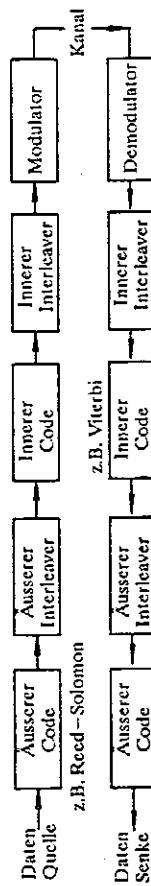


Abb. 4.11 Blockschaltbild des inneren und äusseren Code-Konzepts

1/2 Code“ schaltet man einen Blockverschlachteler (*Interleaver*); oft ist auch ein Blockverschlachteler zwischen innerem und äusserem Code eingefügt.

Abbildung 4.12 zeigt die Leistung marktfähiger *Concatenated Codes* für mittlere Datenraten (*Intermediate Data Rates*; IDR). Mit $E_b - N_0 = 4$ dB werden $BER_{out} = 10^{-8}$ erreicht. Der Gesamt-Code-Gewinn CG beträgt $E_b - N_0 = 12$ dB – CG = 4 dB, also CG = 8 dB.

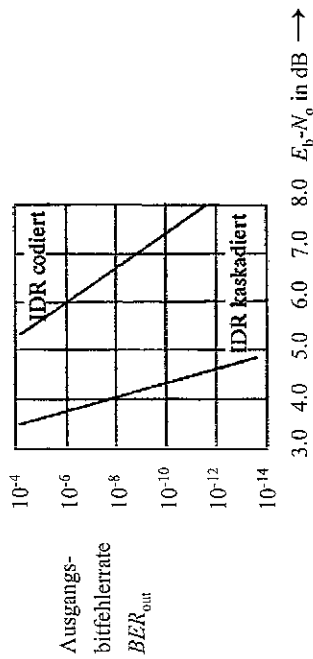


Abb. 4.12 Ausgangsbitfehlerrate BER_{out} gegen $E_b - N_0$ für einfache u. kaskadierte Codierung

Stand der Entwicklung

Die Codiertheoretiker haben in den Siebzigerjahren vergeblich nach dem Universalcode gesucht, der sowohl *Rice Fadings*, wie sie im Mobilfunk auftreten, als auch das Gaussische Rauschen im Festfunk bekämpft.

Sie haben dann in den Achtzigerjahren die Kaskadierung von *Viterbi Codes* (gegen *Rice Fadings*) und *Reed Solomon Codes* (gegen Gaussisches Rauschen) eingeführt, die wir noch heute anwenden. Ende der Neunzigerjahre kam dann der *TurboCode*, der noch höhere „Code Gains“ verspricht als die Kaskadierung von *Viterbi* und *Reed Solomon Codes*, allerdings prozessor- und zeitaufwendiger ist.

Da Prozessoraufwand heute kein Thema mehr ist (die Prozessoren werden immer leistungsfähiger und gleichzeitig billiger), ist das zweifelsfrei die Zukunft.

Turbo Coding

Mit dem Begriff *Turbo Coding* kam 1993 (Claude Berrou und Alain Glavieux) der Durchbruch zur deutlich verstärkten Verarbeitung sowohl von Block-Codes wie auch Sequentiellen Codes in multiplen Stufen, mit denen sich ungleich höhere Codiergewinne erzielen lassen (bis zu 10 dB, bis an das Claude Shannon Limit) für den Preis der Verarbeitungszeit, und diese reduziert sich von Prozessorgeneration zu Prozessorgeneration.

Turbo Coding beruht auf dem Prinzip der *Maximum A Posteriori* (MAP) Wahrscheinlichkeit – was war die wahrscheinlichste Quell-Information.

4.6 Blockverschlachtelung

Codierung ermöglicht die Korrektur einer Anzahl von Übertragungsfehlern. Darüber hinaus kann die Existenz weiterer Fehler angezeigt werden, ohne dass sie jedoch korrigiert werden können. Dabei sind die Codierverfahren umso leistungsfähiger je homogener die Fehler verteilt sind. Es fällt schwer, viele aufeinander folgende Fehler zu korrigieren. Lange Sequenzen falscher Bit können mit dem Blockverschlachteler (*Interleaver*) korrigiert werden. Diese Art von Fehler tritt häufig im Mobilfunk auf. Wenn ein Fahrzeug eine Unterführung durchfährt oder eine Seenotboje von einer grossen Welle abgeschattet wird, sind viele Bit falsch.

Der *Interleaver* besteht aus einem Speicher von n Zeilen und n Spalten, in den das zu übertragende Signal zeilenweise eingelesen wird. Zur Übertragung wird es dann spaltenweise ausgelesen. Empfangsseitig wird das Signal in einen Speicher identischer Struktur spaltenweise eingelesen, um zeilenweise ausgelesen zu werden. Seine ursprüngliche Form ist wieder hergestellt (s. Abb. 4.13).

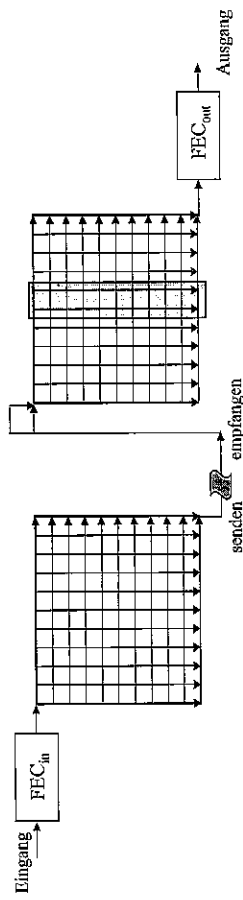


Abb. 4.13 Der Blockverschlachteler

Ein Bündelfehler, der zum Beispiel eine komplette Spalte zerstört (n aufeinander folgende Fehler), streut nach der Spalten/Zeilen-Konversion auf je einen Fehler pro Zeile, der einfach korrigiert werden kann. So können Bündelfehler grosser Länge korrigiert werden. Der Preis dafür ist die Zeitverzögerung, verursacht durch das Einlesen des Send- und Auslesen des Empfangsspeichers. Will man n aufeinander folgende Fehler korrigieren, beträgt die Zeitverzögerung τ bei der Bitrate BR

$$\tau = \frac{2n^2}{BR} \quad (4.16)$$

Dauert die Durchfahrung einer je dreispurigen Autobahn zum Beispiel $\tau = 1,44$ s, dann muss mit $BR = 2$ Mbit/s das $n = \sqrt{1,44 \text{ Mbit/s}} = 1,2$ kbit (der CD-*Interleaver* hat $n = 1,2$ kbit).

Die Methode wird beim digitalen Satellitenhörfunk, der *Compact Disc* (CD) und schon früher bei der magnetischen Aufzeichnung von Bild und Ton verwendet.

Kombination von Codierung und Interleaving

Um die extrem hohe Qualität einer CD und ihren Erhalt auf Jahrzehnte zu ermöglichen, ist die Information zweifach codiert und dreifach blockverschachtelt; die Kaskade von Codier- und Interleaveprozessen ist in Abb. 4.14 dargestellt:

1. Δ -De-Interleaving: geradzahlige Bytes eines Rahmens werden mit den ungeradzahlen des nächsten Rahmens zur Korrektur zufallsverteilter Byte-Fehler und Detektion längerer Bündel-Fehler vertauscht;
2. 28/32-Byte Reed-Solomon C1-Code: zur hauptsächlichsten Fehlerkorrektur wurden nochmals 4 Byte hinzugefügt;
3. Δ^* -De-Interleaving der Bytes: Verteilung der Fehler über mehrere Codewörter; damit können Bündelfehler korrigiert werden, die der Reed-Solomon Code nicht korrigieren kann;
4. 24/28 Byte C2-Parity-Decodierung: 24 Byte sind 4 Parity-Byte zur Fehlerkorrektur beigelegt;
5. Δ -De-Interleaving: Geradzahlige Wertepaare L/R werden von ungeradzahlen separiert, um detektier-, aber unkorrigierbare Fehler durch Interpolation zu verschleiern.



Abb. 4.14 Codierung und Interleaving bei der Compact Disc

Der CD-Decoder vollzieht diese Vorgänge in umgekehrter Folge und stellt das Signalpaar wieder her – selbst wenn einmal ein Kratzer auf der CD ist. Mit Hilfe des Interleaving über 12 000 Bit hinweg und der wiederholten Codierung kann man eine CD, durch die ein 8 mm grosses Loch gebohrt wurde, noch fehlerfrei lesen.

4.7 Modulationsverfahren

Modulationsverfahren werden den Anforderungen der Übertragung und den Störungen auf der Strecke angepasst. Störungen können Rauschen und Funkstörung (Interferenz) sein. Neben der Störresistenz ist Spektrumseffizienz wichtig („... das Frequenzspektrum ist störungsfrei und bandbreiteneffizient zu nutzen“).

Die Fixed Satellite Services (FSS) sind heute durch hohe Effektivleistungen (elektrische Leistung plus Antennengewinn) gekennzeichnet. Damit wurde es Anfang der Achtzigerjahre möglich, mit Einseitenband-Amplitudenmodulation auf Satellitenstrecken höchste Bandbreiteneffizienz zu erzielen: in einem 36 MHz Transponder hat man 18 000 amplitudenkompanierte Telefonkanäle übertragen. Dazu hat man den Telefonkanal, anstatt ihn mit 64 kbit/s zu übertragen, mit 1,7 kHz (im 2 kHz-Raster) analog übertragen. Die Amplitude Companded Single Sideband

⁹ Erster Grundsatz der Frequenznutzungsordnung

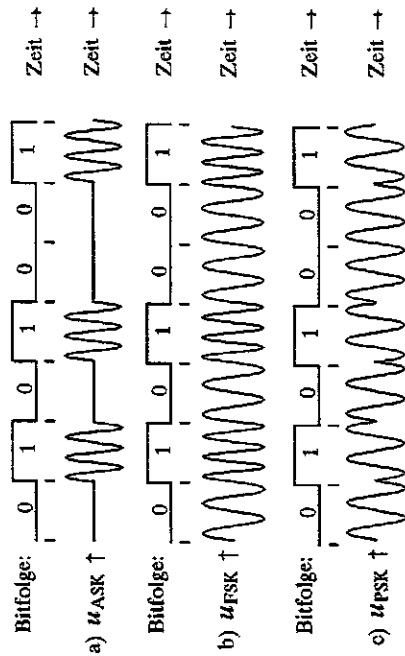


Abb. 4.15 Modulationsverfahren a) ASK b) FSK c) PSK

Suppressed Carrier-Systeme schienen wegen ihrer hohen Demand-Assignment-Flexibilität und ihrer – im Vergleich zu TDMA-Systemen – hohen Wirtschaftlichkeit attraktiv. Dann kam jedoch der digitale Sprachkanal und mit ihm noch höhere Bandbreiteneffizienzen.

Im Mobilfunk steht die Störsicherheit und Zuverlässigkeit der Übertragung im Vordergrund und Bandbreiteneffizienz ist nachrangig (im maritimen Satellitenfunk sind zum Beispiel 0,3 bit/s/Hz durchaus akzeptabel).

Für die Satellitenübertragung haben sich zwei Modulationsverfahren bewährt (s. Abb. 4.15):

- FSK (Frequenzabtaastung/Freq. Shift Keying):

$$u_{FSK} = u_0 \cdot \cos[(\omega_r - \Delta\omega_r) + c(t) \cdot 2\Delta\omega_r] \cdot t$$

- PSK (Phasenumtastung/Phase Shift Keying):

$$u_{PSK} = u_0 \cdot \cos[(\omega_r \cdot t + c(t) \cdot \pi)]$$

Der digitale Nachrichteninhalt $c(t)$ (in Bit) wird in unterschiedliche Amplituden-, Frequenz- oder Phasenzustände des Trägers umgewandelt.

Während in Abb. 4.16 nur zwei Trägersignalzustände gezeigt sind, können es in praxi – bei FSK und PSK – mehrere sein; man spricht dann von MFSK beziehungsweise MPSK, wobei M die Anzahl der Zustände ist. Das Spektrum der 2PSK-Modulation (die Spaltfunktion) gehorcht der Form

$$P(f) = V_0 \left| \int_{-T_{bit}/2}^{+T_{bit}/2} e^{-j\omega t} dt \right|^2 = P_0 \left| \frac{\sin(\frac{\pi f}{f_{bit}})}{\frac{\pi f}{f_{bit}}} \right|^2 \quad (4.17)$$

wobei $f_{bit} = 1/T_{bit}$, T_{bit} die Bit-Dauer ist.

4.7.1 Phasenmodulation

4.7.1.1 QPSK

Abbildung 4.16 zeigt Spektrum und Zeitfunktion von $M = 4$ PSK (Quadrature-PSK). Die Phasenlage des Trägers kann vier Zustände annehmen, wobei pro Phasenlage zwei Bit übertragen werden (vergleiche $M = 2$ PSK). Da QPSK pro Phasenzustand zwei Bit pro Trägerschwingung (Bit/s/Hz) überträgt, wird (für die gleiche Bitrate) gegenüber 2PSK (Bi-PSK oder BPSK) nur die halbe Bandbreite benötigt (s. Abb. 4.17).

Das Spektrum der QPSK-Modulation gehorcht der Form (Baud = Bit pro Zustand)

$$P(f) = V_0 \left[\int_{-\frac{T_{\text{bit}}}{2}}^{+\frac{T_{\text{bit}}}{2}} e^{-j\omega t} dt \right]^2 = P_0 \left[\frac{\sin(\frac{\pi f}{f_{\text{baud}}})}{\frac{\pi f}{f_{\text{baud}}}} \right]^2 \quad (4.18)$$

Die Darstellung der modulierten (und übertragenen) Information in n Bit führt zu der Beziehung mit

$$n = \lg M \quad (4.19)$$

mit $\lg$ dem Logarithmus zur Basis 2; andere Darstellungen führen zu anderen Beziehungen. Informationsgehalt und Bandbreite verhalten sich wie folgt:

Tabelle 4.5 Bandbreiten und Übertragungsraten für verschiedene PSK-Verfahren

M (Zustände)	2	4	8	16	32	64	128	256	512
$n = \lg M$ (Bit/Zustand) ¹²	1	2	3	4	5	6	7	8	
Bandbreite (Hz/Bit) ¹³	1,6	0,8	0,53	0,4	0,32	0,27	0,23	0,2	
Effizienz in (b/s)/Hz	0,63	1,25	1,88	2,5	3,13	3,75	4,38	5	

Das Spektrum der M -PSK-Modulation gehorcht der Form.

Wie aus Abb. 4.18 ersichtlich, muss der Spannungsvektor bei QPSK um $\sqrt{2}$ grösser als der von BPSK sein, für den gleichen Störabstand d zwischen benachbarten Vektoren. Die Leistung des QPSK Symbols muss also um den Faktor 2 grösser als die von BPSK sein. Das QPSK-Symbol transportiert aber 2 Bit statt nur 1 Bit bei BPSK, so dass die Energie pro Bit E_b und damit auch das Verhältnis $E_b - N_0$ von

¹⁰ 64 PSK wurde vor vielen Jahren über Satellit demonstriert; die zögerliche Einführung – trotz der deutlichen Bandbreitenvorteile – beruht auf mangelnder Kenntnis der Nutzer, damit begrenzter Anfrage und damit begrenztem Angebot von Modems

¹¹ 256 PSK wird bei WiMAX (Worldwide Interoperability for Microwave Access) im terrestrischen Funknetz eingesetzt; damit werden 108 Mbit/s in 28 MHz übertragen

¹² Bit/Zustand $\equiv$ Baud

¹³ die Hauptkeule des Spektrums, von Nullstelle zu Nullstelle, ohne Schutzabstand und ohne Codierung

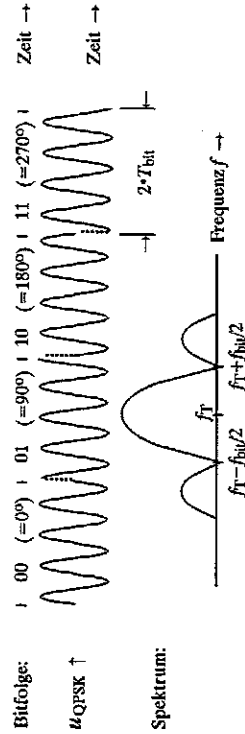


Abb. 4.16 Das Spektrum und die Zeitfunktion von $M = 4$ -PSK (Quadrature-PSK beziehungsweise QPSK)

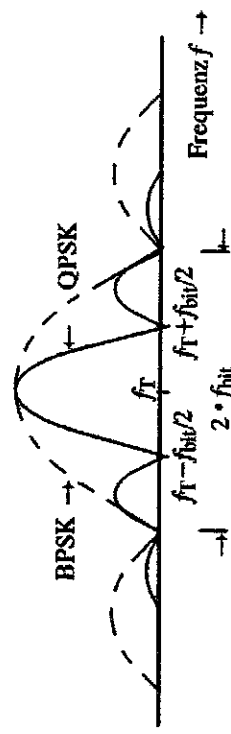


Abb. 4.17 BPSK- und QPSK-Spektren

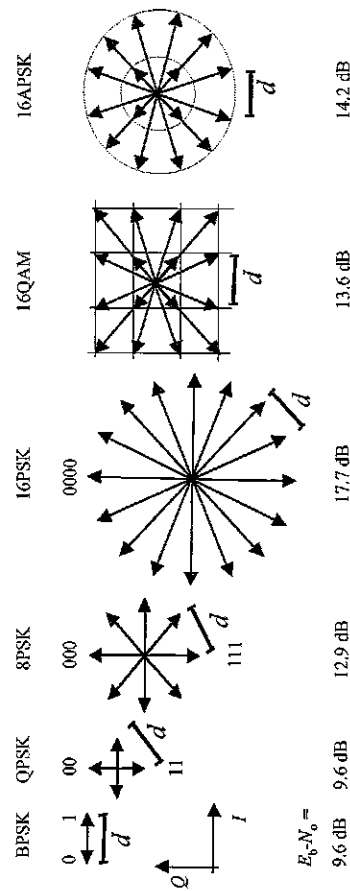


Abb. 4.18 Die „Distanz“ d benachbarter Zustände bei PSK, QAM und APSK

QPSK gleich dem von BPSK ist. QPSK arbeitet mit der gleichen Signalleistung wie BPSK, benötigt aber nur die halbe Bandbreite.

Die Tabelle 4.6 zeigt die $E_b - N_0$ Verhältnisse für verschiedene gängige Modulationsverfahren.

Tabelle 4.6 $E_b - N_0$ vs. BER für verschiedene Modulationsverfahren bei AWGN (in dB)

BER	BPSK ¹⁴	CFSK ¹⁵	FSK ¹⁶	QPSK	8PSK	16QAM	32QAM	64QAM
10^{-1}	-0,9	2,2	5,1	-0,9	2,5	2,2	5,1	11,0
10^{-2}	4,3	7,3	8,9	4,3	7,7	7,3	8,9	12,9
10^{-3}	6,8	9,8	10,9	6,8	10,1	9,8	10,9	13,9
10^{-4}	8,4	11,4	12,3	8,4	11,8	11,4	12,3	14,5
10^{-5}	9,6	12,6	13,4	9,6	12,9	12,6	13,4	15,3
10^{-6}	10,5	13,5	14,2	10,5	13,9	13,5	14,2	16,0
10^{-7}	11,3	14,3	14,8	11,3	14,7	14,5	14,8	16,6
10^{-8}	12,0	15,0	15,5	12,0	15,3	15,0	15,5	17,4
10^{-9}	12,6	15,6	16,0	12,6	15,9	15,6	16,0	18,0
10^{-10}	13,1	16,1	16,5	13,1	16,4	16,1	16,5	18,5
10^{-11}	13,5	16,5	16,9	13,5	16,9	16,5	16,9	19,0
10^{-12}	13,9	16,9	17,3	13,9	17,3	16,9	17,3	19,5
10^{-13}	14,3	17,3	17,7	14,3	17,7	17,3	17,7	20,0
10^{-14}	14,7	17,7	18,0	14,7	18,0	17,7	18,0	20,5
10^{-15}	15,0	18,0	18,3	15,0	18,3	18,0	18,3	20,9

$\gamma = \frac{E_b}{N_0} \quad \kappa = \frac{2\sqrt{\pi\gamma}}{e^{-\gamma}} \quad \kappa = \frac{2\sqrt{\pi\gamma}}{e^{-\gamma}} \quad \kappa = \frac{2\sqrt{\pi\gamma}}{e^{-\gamma}} \quad \kappa = \frac{2\sqrt{\pi\gamma}}{e^{-\gamma}} \quad \kappa = \frac{2\sqrt{\pi\gamma}}{e^{-\gamma}}$

4.7.1.2 OQPSK

Bei versetztem (Offset) QPSK wird der serielle Bitstrom in zwei parallele Ströme „I“ und „Q“ gewandelt und „Q“ um $T/2$ (T = Symboldauer = Bauddauer) verzögert. Durch diesen Versatz werden Amplitudenänderungen auf „von +1 auf 0“ etc. begrenzt; Nulldurchgänge wie „von +1 auf -1“ etc. kommen nicht vor – die „harten“ Zustandsänderungen von „11“ nach „00“ werden vermieden und dadurch die Frequenzbandbreite auf die Hälfte reduziert (erste Nullstellen bei $\pm 0,5T_{\text{baud}}$ anstatt bei $\pm 1,0T_{\text{baud}}$).

4.7.1.3 MSK, GMSK

Minimum Shift Keying (MSK) ist eine Untermenge der PSK-Verfahren (s. Abb. 4.19) kontinuierlicher Phase (Continuous Phase; CP-PSK) und kohärenter Demodulation. Im Gegensatz zum Standard-PSK, das abrupt von einem Phasenzustand zum anderen springt, nimmt sich MSK die Zeit T , einer Symbolperiode, um linear von dem einen Phasenzustand zum anderen zu wechseln.

Das Spektrum der Minimum Shift Keying (MSK) Modulation ist zunächst etwas breiter (der Leistungsabfall ausserhalb der Mittenfrequenz etwas geringer) als das von QPSK, fällt danach aber deutlich weiter ab.

Das Gaussian Minimum Shift Keying (GMSK) wechselt wie der Verlauf einer Gauss-Verteilung vom einen Zustand zum anderen, wobei

¹⁴ κ = BER

¹⁵ kohärentes FSK

¹⁶ inkohärentes FSK

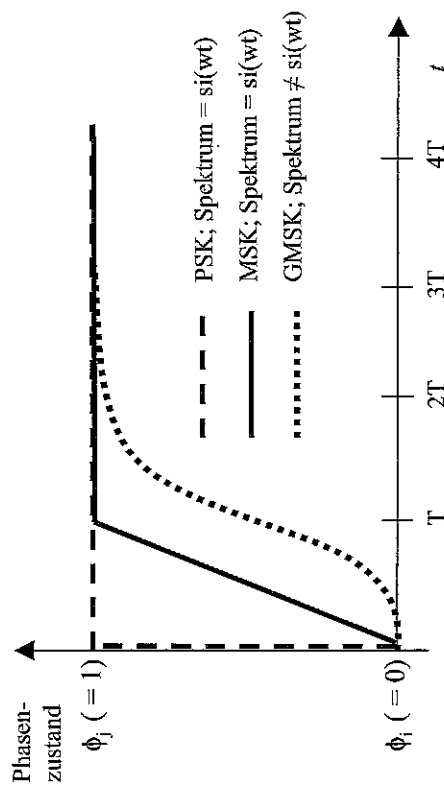


Abb. 4.19 Der Phasenwechsel im Zeitbereich der Modulationsverfahren PSK, MPSK und GMSK

$$d = \Delta f T = 0,5$$

mit Δf = Frequenzhub = $f_2 - f_1$, und $T = 1/f$ = Symbolperiode. Damit ergibt sich ein Spektrum, dessen Hauptkeule bereits schmäler als die aller vorangegangenen Modulationsarten ist, und dessen Nebenkeulen mit f^4 (statt f^2) abfallen, so dass diese Modulation die deutlich spektrumseffizienteste ist.

Die Abb. 4.20 zeigt die Frequenzspektren von QPSK, MSK und GMSK, für $BT' = 0,3$ (im Einsatz im Mobilfunk GSM) und $BT = 0,2$ (kleinste Bandbreitenanforderung).

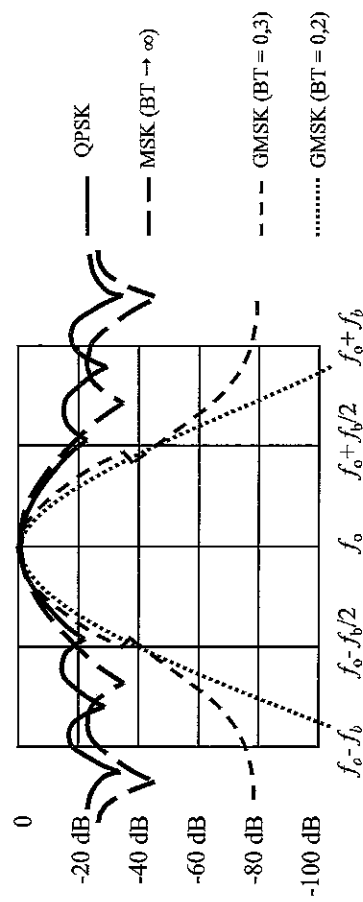


Abb. 4.20 Die Frequenzspektren von QPSK, MSK und GMSK

4.7.1.4 UQPSK, UOQPSK

Neben dem normalen QPSK, das in der In-Phasen-Komponente „I“ und der Quadratur-Komponente „Q“ die gleiche Bitrate transportiert, gibt es „*Unbalanced* QPSK“ UQPSK und UOQPSK, die in den beiden Quadraturkomponenten unterschiedliche Bitraten haben. Ein Beispiel ist GPS, das 50 b/s in „I“ und 1,0 Mb/s in „Q“ überträgt. Einfache Geräte empfangen nur die I-Komponente, professionelle Geräte demodulieren zusätzlich auch die Q-Komponente.

4.7.1.5 BOC, Manchester Modulation

Die jüngst unter der Bezeichnung BOC (*Binary Offset Carrier*) populär gewordene Modulation ist seit langem als die *Manchester Modulation* bekannt. Anstatt der Bitfolge von „1“ und „0“ (NRZ¹⁷), verwendet Manchester die Zustände +1 und -1 in den beiden Bitdauerhälften. Jede der beiden Bitdauerhälften generiert einen Spektralanteil zur Rechten und zur Linken der Trägerfrequenz; auf der Trägerfrequenz ist ein Spektralminimum. Das resultierende Zweifelhörspektrum mit dem Spektralminimum bei der Trägerfrequenz ist in Abb. 4.21 dargestellt:

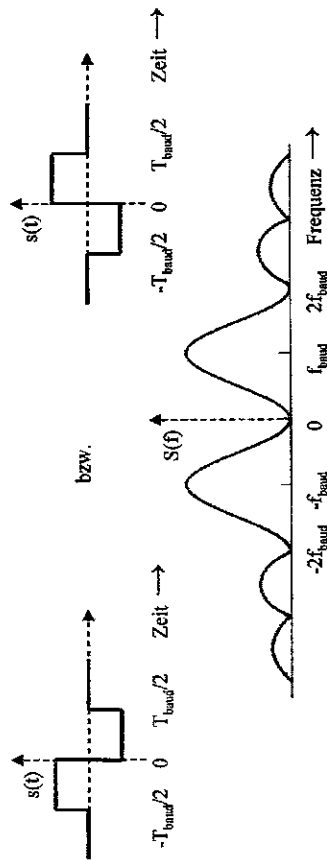


Abb. 4.21 Das Manchester-Zeitsignal und sein Frequenzspektrum

Die gängige Beschreibung des Manchester-Spektrums ist BOC (f_{shift} , chiprate); zum Beispiel hat BOC (15; 2,5) Seitenflügel $f_{\text{shift}} = \pm 15 * 1,023 \text{ MHz} = \pm 15,345 \text{ MHz}$ und die Chiprate „*chiprate*“ 2,5 Mchip/s. Das Spektrum ist von der Form

$$P(f) = P_0 \left[\frac{\sin^4 \left(\frac{\pi f}{2f_{\text{band}}} \right)}{8 \left(\frac{\pi f}{2f_{\text{band}}} \right)^2} \right]^2 \quad (4.20)$$

¹⁷ *Non Return to Zero*, ein Codierungsverfahren für binäre Daten, bei dem das Signal für zwei aufeinander folgende 1en nicht auf den Wert 0 zurückkehrt

Jeder der beiden Seitenflügel nimmt die Bandbreite des entsprechenden QPSK Signals dieser Nutzbitrate ein, da es durch die Multiplikation mit $\text{sign}(\sin(2\omega t))$ ¹⁸ auf die doppelte Übertragungsbitrate angehoben wurde. Dem doppelten Bandbreitenbedarf stand zunächst kein Gewinn entgegen, das Verfahren war ohne Vorteil.

Der Einsatz der Manchester Modulation kam dann im GPS Ortungssystem mit der Forderung, dessen zivilen C/A-Code auf der Mittenfrequenz stören zu können, ohne damit den militärischen P-Code zu stören. Dazu wurde der P-Code Manchester moduliert, sein Spektrum nach rechts und links, ausserhalb des C/A Codes, verlagert (s. Abb. 4.22).

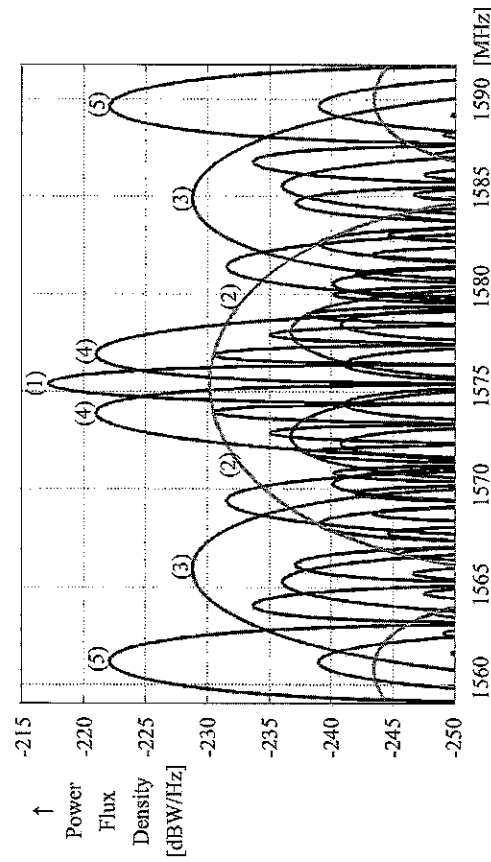


Abb. 4.22 Die BOC-Spektren von GPS und Galileo

Im Bild sind das C/A-Signal von GPS (# 1; BPSK-1), der P(Y)-Code von GPS (# 2; BPSK-10), der M-Code (# 3; BOC 10,5) von GPS, das OS/CS/SAS-Signal von Galileo (# 4; BOC 2,2) und der PRS von Galileo (# 5; BOC 14,2) gezeigt. Die nicht bezeichneten Spektren sind Harmonische der gezeigten Signale. Die endgültigen Signalformen bei Galileo können sich noch ändern.

4.7.1.6 8PSK

Die Modulation mit 8 Phasen (3 bit pro Phasenzustand) statt vier Phasen (und 2 bit pro Phasenzustand) kostet 3 dB mehr $E_b - N_0$ und erhöht den Datenstrom um den Faktor 1,5; um die gleiche Bitrate zu übertragen, benötigt man nur 67% der Bandbreite, verbessert also die Frequenzökonomie. 8PSK-Systeme werden bei VSAT-Netzen und auch bei INTELSAT eingesetzt.

¹⁸ $\text{sign}(x) = 1$ für $x > 0$, $\text{sign}(x) = 0$ für $x = 0$, $\text{sign}(x) = -1$ für $x < 0$

4.7.1.7 QAM, QAMSK

Mit N Phasen und M Amplituden kann man eine grössere Anzahl Z an Zuständen erzeugen, als es mit der gleichen Leistung bei gleichen Amplituden möglich ist. Bevorzugte Konstellationen sind $Z = 16, 64, 256$ etc. Die empfangsseitige Detektion der M Amplituden erfordert gute Amplitudenreinheit, die heute auch auf Satellitenstrecken gegeben ist. Damit wird, in weniger Bandbreite als bei PSK, die Übertragung einer hohen Anzahl von Zuständen (von Bit pro Symbol, also Baud) möglich, bei entsprechend höherer Sendeleistung, die aber in der heutigen Satellitentechnik verfügbar geworden ist.

Die 16QAM Modulation verwendet drei verschiedene Amplituden und zwölf Phasenzustände, um vier Bit pro Symbol zu übertragen. Sie arbeitet mit etwa der Leistung der 8PSK und in der Bandbreite der 8PSK, überträgt aber die 1,33-fache Bitrate.

4.7.2 Puls-Positions-Modulation (PPM)

Bei der Puls-Positions-Modulation moduliert man die Position eines Pulses im Zeitrahmen (s. Abb. 4.23). In speziellen Anwendungen, zum Beispiel in der Ortung, sendet man Pulse zur Bestimmung der Laufzeit des Signals (LORAN; LORAN-C, dem weltweiten Navigationssystem bei 100 kHz). Bei LORAN-C-EUROFIX sitzen die Pulse 1 μ s früher oder später als normal und vermitteln so Information (hier einschliesslich GPS-Korrekturdaten).

Auch das *Downlink* des „Mode S Radar“ bei 1,09 GHz arbeitet mit der Puls-Positions-Modulation (Bitzeit 1 ms).

Die erzielte Bit/Hz-Effizienz wäre für den Kommunikationssektor zu niedrig.

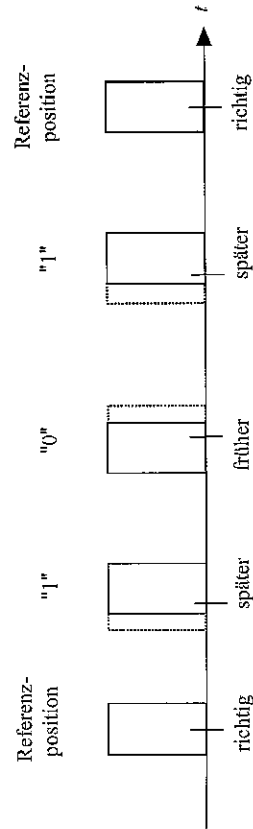


Abb. 4.23 Die Puls-Positions-Modulation

4.7.3 Der Hakenempfänger – Rake Receiver

Beim Empfang von Funksignalen stellt sich immer das Problem, dass sich Komponenten des gewünschten Signals von der Erdoberfläche oder Gebäuden etc. reflektieren und nach diesem Mehrweg in die Antenne gelangen, wo sie zusätzlich zum gewünschten Signal empfangen werden, und zwar umso gleichwertiger je kleiner

die Richtwirkung der Antenne ist. Die Richtwirkung der Antenne schwindet mit der Grösse (der Apertur) und ist gleich Null bei rundumstrahlenden Antennen wie sie zum Beispiel im Mobilfunk-Handy verwendet werden.

Auf Grund des Mehrweges dieser Streusignale („Echos“) sind sie nicht in Phase mit dem gewünschten Signal. Ihre Überlagerung mit dem gewünschten Signal verursacht eine Signalstörung. Im schlimmsten Fall, wenn sie 180° phasenversetzt sind, löschen sie das gewünschte Signal teilweise oder ganz aus; sie verursachen einen Signalschwund („*Multipath Fade*“).

In der (vergangenen) Zeit der analogen Übertragung gab es keine Möglichkeit, diesen Mehrweg-Effekt („*Multipath Effect*“) zu vermeiden oder wenigstens zu lindern, ausser, wenn es möglich war, Antennen grosser Apertur zu verwenden, was mindestens im Mobilfunk nur begrenzt möglich ist.

Auch die Erhöhung der Sendeleistung, wie immer wieder zur Mitigierung der Mehrweg-Störung gefordert, ist natürlich falsch, da die Leistung des Mehrweg-Signals mit der Leistung des gewünschten Signals steigt oder fällt; sie ist nur um den Reflektionsverlust kleiner als die des gewünschten Signals, und dieser ist unabhängig von der Sendeleistung.

Die Ingenieure Price und Green^{19, 20} haben bereits 1955 an der intelligenten Verarbeitung digitaler Signale gearbeitet. Das Ergebnis war ein Empfangssystem bestehend aus einem Hauptempfänger und mehreren Nebeneempfängern, die in ihren Phasenlagen zum Hauptempfänger versetzt liegen und die Mehrwege-Signale per Korrelation detektieren und so verarbeiten (in ihren Phasenlagen zurechtrücken), dass sie zum Hauptsignal hinzugefügt (in der Spannung zum Summensignal addiert) werden können. Damit werden die Signalspannungen kohärent addiert, die (unabhängigen) Rauschspannungen jedoch inkohärent, so dass sich das Signal/Rausch-Verhältnis (und das $E_b - N_0$) ebenfalls verbessert.

Die Mehrweg-Signale stören nicht mehr sondern verbessern sogar die Qualität des gewünschten Signales. Man kann den Hakenempfänger sogar als *Diversity Receiver* verstehen: Der Empfang wird durch die diversitären Signale solidifiziert. Im Limit ist es denkbar, dass der Empfang durch die multiplen Echos aufrecht erhalten bleibt, wenn das Direktsignal ausfällt.

Man kann sich die (zum Beispiel 16) Untereempfängerzüge und das (eine) Summensignal wie die Zinken beziehungsweise den Stil einer Harke vorstellen (s. Abb. 4.25) – daher „Hakenempfänger“, die Substantiv-Erklärung für diese Bezeichnung. Die Verb-Erklärung der Vokabel, die bereits von Price und Green stammt, könnte sein, dass das Gerät die Einzelkomponenten wie ein Rechen zusammen harkt.

Da das Direktsignal um die zusätzliche Laufzeit des Echos verzögert werden muss, damit das Echo in Phase hinzu addiert werden kann, entsteht eine Signalverzögerung um den Betrag der zusätzlichen Laufzeit (einige μ s). Diese Latenz ist im Mobilfunk ohne Bedeutung und bei Satellitenverbindungen ohnehin relativ

¹⁹ R. Price and P.E. Green, „*A communications technique for multipath channels*“, US-Patent, 1956

²⁰ R. Price and P.E. Green, „*A communications technique for multipath channels*“, *Proceedings of the IRE*, Vol. 46, pp. 555–570, March 1958

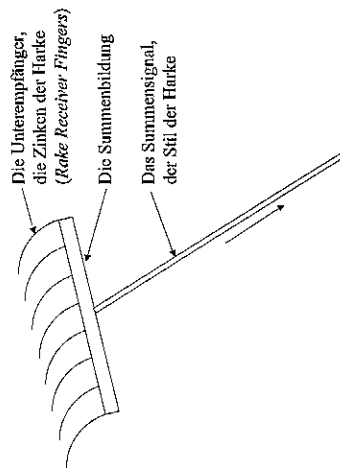


Abb. 4.24 Die prinzipielle Architektur des Hakenempfängers

zur Satellitenlaufzeit ($\approx 1/4$ s) vernachlässigbar; sie sollte aber in einem Navigationsempfänger nicht vernachlässigt werden; dort bedeuten 3 μ s Verzögerung einen Fehler von 1 km.

Rake-Empfänger werden heute in Mobilfunksystemen, satellitengestützt (GlobalStar etc.) als auch terrestrisch (I-95, das „D-Netz“ in USA etc.) eingesetzt.

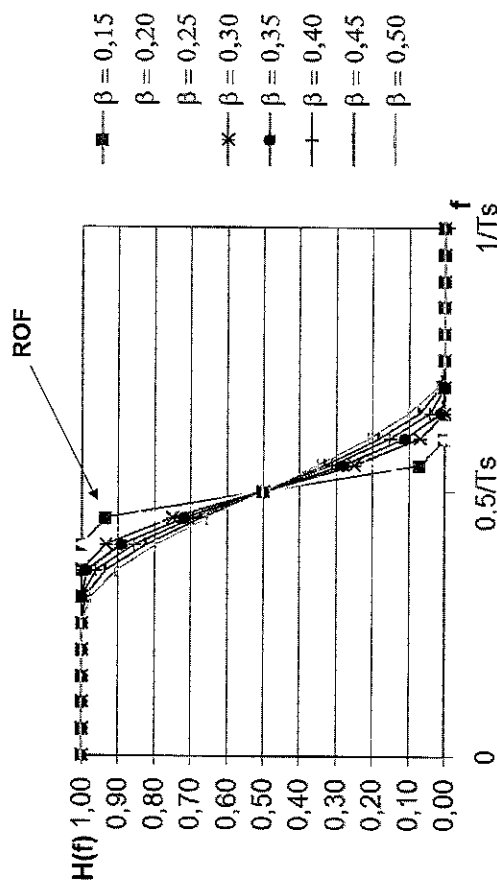
4.7.4 Spektralabfall der PSK-Modulation – Der Roll-Off Factor

Der spektrale Abfall eines PSK modulierten Signales (der *Roll-Off Factor*) ist das Mass für die Nutzung des Spektrums. Je steiler das Spektrum eines Hochfrequenzträgers beginnend von der Mittenfrequenz des Trägers abfällt, desto enger können die Träger angeordnet werden, desto besser ist die Bandbreitennutzung. Die Hauptkeule des Spektrums eines (digitalen) BPSK-Signales ist $f = 2/T_s$ breit (s. Abb. 4.25), 50% der Leistung ist aber im Band $f = 1/T_s$ konzentriert.

Durch geeignete Filterung des Hochfrequenzträgers, der so genannten Nyquist-Filterung des Signales, wird der Abfall des Spektrums ausserhalb $f = 1/T_s$, also $f = +0,5/T_s$, sehr steil, so dass nur wenig mehr als $f = 1/T_s$ pro Träger vorgesehen werden muss.

Der Frequenzgang des Nyquist-Filters ist gegeben durch

$$H(f) = \begin{cases} \frac{T_s}{2} \left\{ 1 + \cos \left[\pi \cdot T_s \left(|f| - \frac{(1-\beta)}{2 \cdot T_s} \right) \frac{1}{\beta} \right] \right\} & \text{für} \\ 0 \leq |f| \leq \frac{1-\beta}{2T_s} \\ \frac{1-\beta}{2 \cdot T_s} \leq |f| \leq \frac{(1+\beta)}{2 \cdot T_s} \\ |f| > \frac{(1+\beta)}{2 \cdot T_s} \end{cases} \quad (4.21)$$

Abb. 4.25 Der Roll-Off Factor für $\beta_{ex}(0,15; 0,50)$ gegen die Frequenz

Hier ist β der *Roll-Off Factor* (ROF). Abbildung 4.25 zeigt den Spektralabfall für *Roll-Off Factors* $\beta = 0,15$ (die steilste Kurve) bis $\beta = 0,50$ (die am wenigsten steile Kurve) gegen die Frequenz f , gemessen von der Trägermittenfrequenz f_0 bis $f_0 + T_s$. Für $\beta = 0$ ist der ROF bis $f = f_0 + 0,5/T_s$ gleich 1,0 und springt dort auf 0,0 vertikal ab.

Gängige machbare *Roll-Off Factors* in der Praxis sind

$\beta = 35\%$ (DVB-S Standard; 36 Mb/s QPSK in 36 MHz)

$\beta = 20\%$ (DVB-S2 Standard; 54 Mb/s QPSK in 36 MHz)

$\beta = 15\%$ (INTELSAT-TDMA, 1974; 64 Mb/s QPSK in 36 MHz).

In erster, grober Näherung kann man die benötigte Hochfrequenzbandbreite BW in Abhängigkeit des *Roll-Off Factors* wie folgt ansetzen:

$$BW = \frac{0,5(1+\beta)}{T_s} \quad (4.22)$$

Ausgedrückt in der zu übertragenden Bitrate BR wird die Näherungsgleichung zahlenmässig zu

$$BW = 0,5 \cdot BR (1 + \beta) \quad (4.23)$$

Da Satelliten-Transponderbandbreite Geld kostet, ist es sinnvoll, einen Spektralabfall von mindestens $\beta = 0,20$ bzw. 20% entsprechend dem internationalen DVB-S2 Standard einzusetzen – siehe Beispiel.

Beispiel: Für die Übertragung von $BR = 100$ Mb/s ergibt sich so ein Bandbreitenbedarf von $BW = 0,5 \cdot 100(1 + 0,20) = 60$ MHz. Hinzu sollte man bei Mehrträgerbetrieb im Transponder ca. 10% der Bandbreite als Schutzabstand zu den Nachbarträgern einräumen (je 5% zur Rechten und zur Linken); in Summe müssen 66 MHz angesetzt werden.

4.7.5 Codulation

Die *Codulation* verknüpft die Modulation mit der Kanalcodierung. Wie kann die Codierung des Bitstroms präpariert werden, um im Verbund mit der Modulation auf die Unwirren des Kanals unbeschadet zu überstehen? Die Modulation kann demodulatorfreundliche Attribute beinhalten wie zum Beispiel die Vermeidung benachbarter Bitfolgen in aufeinander folgenden Zeichen; war das letzte Symbol die Bitfolge 010, sind die Bitfolgen 110, 000 und 011 ausgeschlossen; diese a priori Information unterstützt den Entscheidungsprozess des Demodulators und mindert so die Bitfehlerwahrscheinlichkeit.

Eine bewährte Codulation ist auch die *Trellis Coded Modulation* (TCM), ein konventionelles Modulationsverfahren im Verbund mit Faltungscodierung.

Die Codierung benötigt hierbei – wie jede Codierung – zusätzliche Bit über die Informationsbit hinaus; die Modulation mit zum Beispiel 8PSK anstatt 4PSK benötigt eine höhere Leistung, erhöht aber auch die Bitrate. Diese zusätzliche Bitrate ermöglicht die Codierung. Der erzielte Codiergewinn des Faltungscodes übersteigt die zusätzliche Leistungsforderung des höherwertigen Modulationsverfahrens.

Die Übertragung der höheren Bitrate findet in der gleichen Bandbreite (des ursprünglichen 4PSK) statt.

► TCM spart Sendeleistung ohne Erhöhung der Bandbreite.

Im Beispiel ist das Träger/Rauschleistungsverhältnis für die 8PSK um 3 dB höher als für die 4PSK Modulation; der Codiergewinn des Rate 2/3 Faltungscodes beträgt 5 dB; der Nettogewinn ist also 2 dB.

4.7.6 Systemtechnischer Vergleich der Modulationsverfahren

Die Modulationsverfahren unterscheiden sich in ihrer Eignung und Fähigkeit, Signalqualität für Übertragungsleistung in einer begrenzten Bandbreite zu liefern. Abbildung 4.26 zeigt die Signalqualität in $S-R$ gegen die Träger/Rauschleistung $C-N$ für Amplitudenmodulation (auch für $C = N$ ist $S = R$ noch demodulierbar), für Frequenzmodulation und *Threshold Extension* FM (TEFM; hoher Modulationsgewinn gegenüber AM, aber – im Gegensatz zu AM – eine $C-N$ -Schwelle, unterhalb der Demodulation nicht mehr möglich ist) und für digitale Modulation, die gegenüber FM wesentliche Möglichkeiten der Qualitätsverbesserung beinhaltet, aber eine noch härtere Schwelle besitzt, bei der der Demodulator „aussteigt“.

Ein wesentlicher Unterschied zwischen FM und PSK ist, dass das FM-Spektrum mit der Gauss-Verteilung abnimmt, während PSK gemäß Gleichung 4.13 die $(\sin x/x)^2$ -*Sidelobes* aufweist. Mit der GMSK-Modulation kann die Gauss-Verteilung des Spektrums aber auch in der digitalen Übertragung erreicht und erhalten werden.

Die *Sidelobes* der PSK-Modulation lassen sich nämlich zwar sendeseitig bandpassfiltern, sie treten aber in jedem Folgeglied wieder auf²¹.

²¹ „... du magst die Natur mit der Mistgabel austreiben, sie kehret doch zurück!“ (*naturam furcu expellas, tamen usque recurrit*; Horaz, ep. I 10,24.)

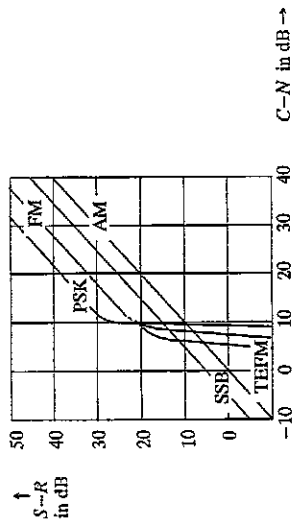


Abb. 4.26 Signalqualität gegen Übertragungsleistung in $C-N$ für einige Modulationsverfahren

Über den Einzelthemen der Technologie und den Verfahren steht das *System Engineering* als eigenständige Ingenieurdisziplin und ist von grundlegender Bedeutung. Es definiert das Gesamtsystem aufgrund der Anforderungen und erarbeitet dann, wie das gestreckte Ziel am betriebswirtschaftlichsten erreicht werden kann. Bei einem Fernmeldeprojekt versucht der Systemingenieur für die Definition des Leistungsprofils

1. die Übertragungskapazität maximal zu nutzen,
2. die Übertragungsqualität zu garantieren,
3. Parameter wie Laufzeit, Interferenz, Zuverlässigkeit etc. zu berücksichtigen,
4. Randbedingungen wie Satellitenorbit, verfügbare Leistung, Systemreserve einzuhalten,
5. die Kosten des Systems und seines Betriebs zu minimieren.

Hierbei stehen zum Beispiel die Ziele 2. und 5. im klassischen Widerspruch. An dieser Stelle unterscheidet man Systemparameter, die gegeneinander verhandelt werden können (*Trade-Offs*) und systembegrenzende Vorgaben durch die Physik, die rechtliche oder betriebsrechtliche Situation oder durch die vorgegebene Finanzdecke des Projektes. Physikalische Grenzen sind zum Beispiel:

- das Nyquist-Theorem für die Übertragungsbandbreite
- das Shannon-Limit für die Übertragungskapazität.

Rechtliche und betriebsrechtliche Randbedingungen sind:

- die regulatorische Situation des Betriebs von Fernmeldeanlagen
- die betriebsrechtlich festgelegte Nutzung von Funkfrequenzen
- zu Orbitzuordnungen
- die Funkstörung (Interferenz) mit anderen Anlagen.

Die Aufgabe des Systemingenieurs ist, in Kenntnis der verfügbaren Technologie, der möglichen Verfahren und der rechtlichen Möglichkeiten ein System auszulegen, das die größtmögliche Fernmeldekazität am wirtschaftlichsten beisteht. Von dieser Warte aus werden Untersysteme definiert.

Die umgekehrte Vorgehensweise, die für die diversen Subsysteme und Komponenten verantwortliche Ingenieure nach eigenem Gusto ihre Geräte perfektionieren

zu lassen, führt zu hohen Kosten für das Gesamtsystem. Die Einsparung von 1 dB Sendeleistung – als eines von vielen *Trade-Off*-Beispielen – kann wahlweise erreicht werden durch:

- | | |
|--|--------------------------------------|
| höheren Sendeanhengewinn | höheren Empfangsantennengewinn |
| kleinere Empfänger-Rauschleistung | kleinere Streckenverfügbarkeitsmarge |
| kleinere Übertragungskapazität | niedrigere Übertragungsqualität |
| höhere Übertragungscodierung | bessere Quellencodierung oder |
| kleinere Verluste zwischen Sender und Antenne. | |

Jede Alternative bietet andere Abhängigkeiten, Sekundäreffekte und Kostenauswirkungen. Folglich kann die Entscheidung, von welchen Subsystemen beziehungsweise Systemparametern das fehlende dB zu erbringen sei, vom *System Engineer* nur unter Berücksichtigung der Möglichkeiten, Durchführbarkeiten (zum Beispiel der Qualitätsreduktion), Abhängigkeiten (zum Beispiel des Antennengewinns von der Richtwirkung und Bedeckungszone) und der jeweiligen Kosten, für Entwicklung, Herstellung, Betrieb und Ausmusterung gefällt werden.

Trade-Offs von Leistung und Bandbreite können, wie schon in der analogen Frequenzmodulation Leistung gegen Bandbreite gegeben werden (je höher die Leistung, desto kleiner die Frequenzbandbreite): Auch bei der digitalen Modulation kann Leistung gegen Bandbreite getauscht werden. Je höher die verfügbare Leistung, desto höherwertige Modulationsverfahren können verwendet werden, die umso weniger spektrale Bandbreiten einnehmen.

Wichtig ist, dass man mit Technologie Übertragungsbandbreite sparen kann. Das Pendant zu den *Threshold Extension* Demodulators der analogen Frequenzmodulation sind in der digitalen *Phase Shift Keying* heute die höherwertigen Modulationsverfahren mit 4, 16, 64 etc. Phasenzustände.

► Die Bandbreite geht mit der Frequenz der Phasenwechsel – der Baud-Rate.

Für die Baud-Rate 100 und den ROF 0,20 werden 60 Hz benötigt, unabhängig davon, ob jedes Baud 1 Bit transportiert (BPSK) oder 64 (64QAM). 64QAM ist aber sechs Mal effizienter.

Der *Trade-Off*-Bereich von Leistung und Bandbreite bei digitalen Übertragungen zum Beispiel lässt sich mit dem Shannon-Theorem abgrenzen:

4.7.7 Die benötigte Bandbreite im Satelliten

Wie ermittelt man die Bandbreite im Satelliten, die zur Übertragung eines Dienstes benötigt wird? Die Satellitenbandbreite hängt ab von:

- der zu übertragenden Bitrate des Dienstes
- der verwendeten Formatierung
- dem vom Nutzer ausgewählten Modulationsverfahren
- dem oder der eingesetzten Codierverfahren, FEC oder RS oder FEC&RS etc.
- der Anzahl der zu übertragenden Einzelträger des Nutzers
- dem Schutzabstand zwischen den Einzelträgern, zum Beispiel 10% der Bandbreite

Die Ermittlung lässt sich am besten mit einem Beispiel erläutern: Es sollen 2,048 Mbit/s zwischen A und B ausgetauscht werden.

Der zu übertragende Bitstrom (Punkt i) ist also 2,048 Mbit/s; wenn zum Beispiel in einem TDMA Rahmen formatiert wird (Punkt ii), kommen ca. 10% Rahmendaten hinzu, so dass die zu übertragende Brutto-Bitrate 2,26 Mbit/s beträgt.

Wird nun das Modulationsverfahren QPSK ausgewählt (Punkt iii), dann entnimmt man der Tabelle 4.5 für $M = 4$ den Bandbreitenwert 1,27 MHz pro Mbit/s; für 2,26 Mbit/s also 2,87 MHz.

Soll der Bitstrom für die sichere Übertragung mit, zum Beispiel, FEC Inner Code der Rate $3/4$ und zusätzlich mit *Reed-Solomon Outer Code* der Rate $204/188$ codiert werden (Punkt iv), ergibt sich die Summenbitrate $2,87 / (3/4) / (188/204)$ MHz = 4,15 MHz.

Für die Duplexverbindung A nach B plus B nach A benötigt man zwei Einzelträger (Punkt v); hierfür werden 8,3 MHz benötigt – noch ohne Schutzabstand.

Zwischen den beiden Einzelträgern, insbesondere aber auch unterhalb und oberhalb des Trägerpaares, muss zwingend ein Schutzabstand (Punkt vi) vorgesehen werden, um die Störung der benachbarten Träger in Grenzen zu halten (Träger stören die Nachbarträger und werden ihrerseits auch von den Nachbarträgern gestört, wenn man sie zu dicht packt). Mit zum Beispiel 10% Schutzabstand je zur Rechten und zur Linken eines Trägers wird die insgesamt benötigte Bandbreite dann $8,3 \text{ MHz} + 3(4,15 \text{ MHz } 0,1) = 9,55 \text{ MHz}$.

Gibt der Satellitenbetreiber Bandbreiten in ganzzahligen Vielfachen von zum Beispiel 1 MHz ab, müssen für die vorliegende Übertragung 10 MHz angemietet werden.

4.8 Frequenzumsetzung

Die Umsetzung des sendeseitigen Modulatorausgangs (zum Beispiel 1,5 GHz) auf die *Uplink*-Frequenz (zum Beispiel 14 GHz), die Umsetzung der *Uplink*-Frequenz auf die *Downlink*-Frequenz im Satelliten (zum Beispiel 11 GHz) und die Umsetzung der *Downlink*-Frequenz auf die Demodulator-Eingangsfrequenz im Empfänger geschieht mit Hilfe eines Mischers, der von einem Oszillator beaufschlagt wird (s. Abb. 4.27). Das Ergebnis ist ein Ausgangssignal $f_2 = f_1 \pm f_{\text{Mixer}}$. Nachfolgend wird

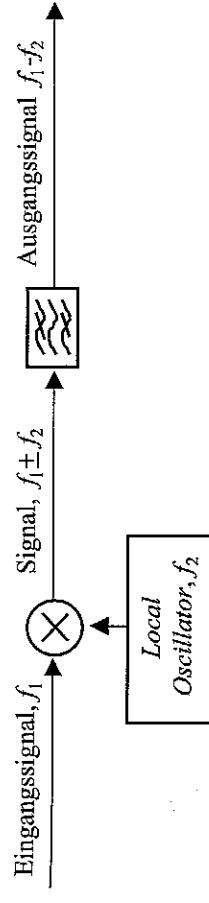


Abb. 4.27 Der Frequenzumsetzer (Up-Converter, Down-Converter)

das gemischte Signal bandpassgefiltert, um die spiegelsymmetrische Komponente $f_1 + f_{\text{Mixer}}$ zu stoppen; der Ausgang des Frequenzumsetzers ist dann $f_2 = f_1$.

Im Satelliten ist die Frequenzumsetzung konstant über die Lebensdauer des Satelliten; es wird ein starrer *Local Oscillator* verwendet. Die Endgeräte am Boden müssen so ausgelegt werden, dass sie jederzeit ohne Montageeingriff auf eine beliebige Frequenz in irgendeinem der Transponder des Satelliten eingesetzt werden können. Dazu sind sie mit flexiblen Oszillatoren (*Frequency Agile Oscillators*) ausgestattet.

In Endgeräten am Boden, die heute weitestgehend in Software ausgelegt sind („*Software Radio*“), wird auch die Frequenzumsetzung in Software realisiert.

4.9 Die Übertragung

4.9.1 Die Übertragungskapazität – das Shannon Limit

Wie wird die Kanalkapazität (die Bitrate der Übertragung oder Übertragungsrate in b/s) cc durch die Bandbreite bw (in Hz) und das Rauschen n (in W) begrenzt:

$$cc = bw \cdot \lg_2 \left(1 + \frac{s}{n} \right) \quad (4.24)$$

mit s der Signalleistung in W. Dies ist das *Shannon Limit*, von Claude Shannon, einem Ingenieur der *Bell Telephone Laboratories* in Murray Hill, N.J., im Jahr 1948 veröffentlicht.

Die Wandlung von $\lg_2$ nach $\ln_e$ ergibt

$$cc = bw \cdot 1,44 \ln_e \left(1 + \frac{s}{n} \right)$$

In dieser Form lässt sich der Grenzwert für $s/n \ll 1$ bestimmen zu

$$cc = bw \cdot 1,44 \frac{s}{n}$$

bzw.

$$\frac{s}{n} = \frac{1}{1,44} = 0,69$$

Mit der Wandlung nach $\log_{10}$ ergibt sich die Form in dB:

$$(S - N) - (CC - BW) = -1,6 \text{ dB, der Grenzwert für } s/n \ll 1,$$

mit $CC = 10 \log(cc)$, $BW = 10 \log(bw)$, $S = 10 \log(s)$ und $N = 10 \log(n)$.

Mit der Signalenergie pro Bit E_b zu Rauschleistungsdichte N_0 und $E_b - N_0 = S - N$ ergibt sich

$$(S - N) - (CC - BW) = (E_b - N_0) - (CC - BW) = -1,6 \text{ dB.} \quad (4.25)$$

Für $s/n > 1$, also der Normalfall, gilt,

$$\frac{cc}{bw} = \lg_2 \left(1 + \frac{s}{n} \right).$$

Mit der Wandlung nach $\log_{10}$ ergibt sich die Form in dB:

$$\begin{aligned} CC - BW &= 10 \log_{10} \left[\lg_2 \left(1 + \frac{s}{n} \right) \right] \\ &= 10 \log_{10} \left[3,322 \log_{10} \left(1 + \frac{s}{n} \right) \right] \\ &= 5,2 + 10 \log_{10} \left[\log_{10} \left(1 + \frac{s}{n} \right) \right] \end{aligned} \quad (4.26)$$

Diese Funktion von $CC - BW$ gegen s/n beziehungsweise $E_b - N_0$ ist in Abb. 4.28 gezeigt, vom linken Grenzwert für $E_b - N_0 = -1,6 \text{ dB}$, dann der Nulldurchgang mit $CC - BW = 0 \text{ dB}$ für $E_b - N_0 = 0 \text{ dB}$, bis ca. $E_b - N_0 = 20 \text{ dB}$. Unterhalb dieser Kurve liegt der realisierbare Bereich, die Kurve selbst stellt den Grenzfalle der Bitfehlerrate 0,5 dar, und oberhalb der Kurve ist der nichtrealisierbare Bereich.

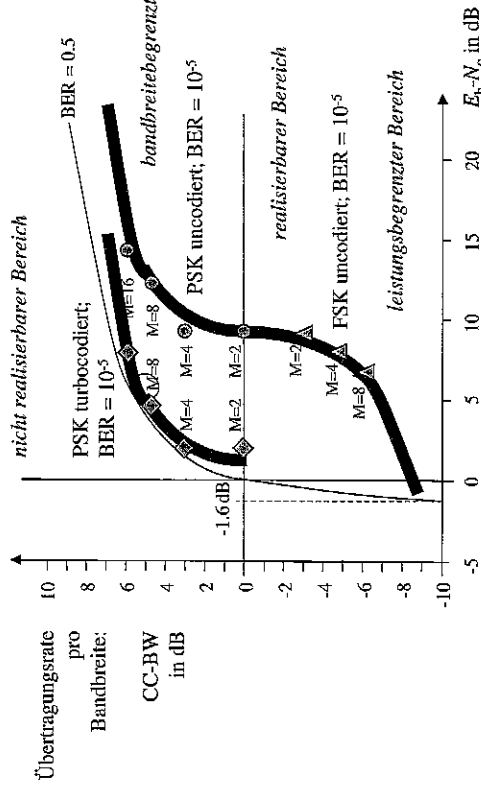


Abb. 4.28 Übertragungsrate CC über Bandbreite BW gegen $E_b - N_0$

In diesem Graph kann man für ein vorgegebenes $E_b - N_0$ das maximal erreichbare $CC - BW$ ablesen, beziehungsweise für ein gefordertes $CC - BW$ das notwendige $E_b - N_0$.

Von links unten in Richtung nach rechts oben werden diverse Modulationsverfahren durchschritten, die zunehmende Verbesserung bringen (zum Beispiel von inkohärentem FSK über kohärentes FSK, differentielles PSK, kohärentes PSK etc., alle $M = 2$), alle für $BER = 10^{-5}$.

Im realisierbaren Bereich sind vier M-PSK Modulationsverfahren ($M = 2, 4, 8$ und 16) mit einer Bitfehlerrate von 10^{-5} und drei M-FSK Modulationsverfahren ($M = 2, 4$ und 8), ebenfalls mit einer Bitfehlerrate von 10^{-5} eingetragen.

Die obere Halbebene mit $CC-BW > 0$ dB ist der bandbreitenbegrenzte Bereich, für $CC-BW > 0$ dB ist die Übertragung leistungsbegrenzt.

Bemerkenswert ist, dass die Phasenmodulation (*Phase Shift Keying*; PSK) mit vier Phasen ($M = 4$) für das gleiche $E_b - N_0$ um 3 dB höhere $CC-BW$ zeigt (die doppelte Übertragungsrate pro Bandbreite) als das 2-Phasen PSK.

Die Frequenzsprungmodulation (*Frequency Shift Keying*; FSK) mit zwei Frequenzen ($M = 2$) zeigt hier für das wiederum gleiche $E_b - N_0$ um 3 dB niedrigere $CC-BW$ (nur die halbe Übertragungsrate pro Bandbreite) im Vergleich zu 2-Phasen PSK. Die Frequenzsprungmodulation mit vier Frequenzen ($M = 4$) zeigt sogar, für das gleiche $E_b - N_0$, um 6 dB niedrigere $CC-BW$ (nur ein Viertel der Übertragungsrate pro Bandbreite) im Vergleich zu 2-Phasen PSK.

Man wird dieses bandbreitenineffiziente Modulationsverfahren (FSK) also nur dort einsetzen, wo die Robustheit seiner Demodulation gefordert ist (es ist technisch einfacher, eine Frequenz im Spektrum zu detektieren als die Phasenlage eines Hochfrequenzträgers zu bestimmen).

Der Kurvenverlauf links oben zeigt die PSK-Performance im Verbund mit Turbocodierung. Die $E_b - N_0$ -Werte liegen unmittelbar neben dem Shannon-Limit, der Abstand maximal möglichen Übertragungskapazität („*Close the gap to capacity!*“).

In der Satellitenkommunikation ist man seit langem nicht mehr leistungsbegrenzt sondern bandbreitenbegrenzt und greift deshalb zu PSK-Modulation mit immer höherwertigen Phasenzuständen (16-QAM, 64-QAM, 256-QAM etc.).

Generell gilt: Höhere Bandbreiteneffizienz ist notwendig. Nur im Mobilfunk und insbesondere im leistungsbegrenzten SAR wird man weiterhin das robustere, leistungsparsamere, weniggleich bandbreitenaufwendigere FSK verwenden.

4.9.2 Kanalabhängige Bitrate, Codierung und Modulation

Seit vierzig Jahren sind Geräte mit variabler Bitrate verfügbar, die sich dem Kanalzustand anpassen. Wenn der Decodierer eine hohe Bitfehlerrate zurück meldet, reduziert der Sender die Bitrate entsprechend, so dass mit der aktuellen (reduzierten) Leistung der kleinere Bitstrom fehlerfrei übermittelt werden kann. Nach Beendigung des Signalschwundes wird die Bitrate wieder auf den nominalen Wert angehoben.

Diese „*Variable Bit Rate*“ (VBR) Geräte werden inzwischen auch im Satellitenfunk eingesetzt; „Lieber langsam als schlecht“, es ist besser, die Übertragungsdauer geringfügig zu erhöhen als sich unzulässig viele Fehler einzuholen.

Eine weitere Verbesserung der Übertragungsqualität kann erreicht werden, wenn man, in der Bereitschaft, etwas mehr Übertragungsdauer zuzulassen, den Codierungsaufwand erhöht, von, zum Beispiel, einer Rate $3/4$ auf die Rate $1/2$. Damit erreicht man etwa 2 dB mehr Codiergewinn, und die Nachricht oder die Daten sind besser geschützt. Dies ist die kanalabhängige Codierung.

Ähnlich passt man auch das Modulationsverfahren an den Kanalzustand an; man überträgt mit 16-QAM solange die Kanalqualität es zulässt und fällt auf das robuste (aber langsamere) QPSK zurück, wenn Schwunderscheinungen auf dem Kanal auftreten. Dies ist die kanalabhängige Modulation.

Schliesslich setzt man heute kanalabhängige Übertragungsprotokolle wie das *Hybrid Automatic Repeat reQuest* (HARQ) ein, die auf der Basis einer *Forward Error Correction* (FEC) nicht in den Übertragungsablauf eingreifen, so lange der Decoder mit dem empfangenen Signal zurechtkommt. Übersteigt die Bitfehlerrate aber einen Grenzwert, wird auf *receive Acknowledgement* (ACK, eine Bestätigung nach jedem Rahmen) oder besser auf *Negative receive Acknowledgement* (NACK, Rückmeldungen, nur wenn ein Rahmen nicht decodierbar war) übergegangen.

4.10 Zusammenfassung

Die Kanal-Codierung spart Sendeleistung: 6 dB Codiergewinn für nur 3 dB mehr Bandbreite viertelt die Sendeleistung und senkt die Übertragungskosten. Zur Anpassung an mehrere Kanalzustände lassen sich mehrere Codes kaskadieren. Turbocodes zerteilen die notwendige Übertragungsleistung (auf -10 dB).

Die Blockverschachtelung eliminiert Blockfehler (viele Fehler in Serie, im Gegensatz zu stochastischen Einzelfehlern) grosser Länge ohne zusätzliche Codierbits – ohne die Bitrate zu erhöhen; sie sollte grosszügig genutzt werden.

Chiffrierung ist notwendig. Der Wettbewerber hört mit (*Eaves Dropping*) und verändert eventuell die Information zu unserem Nachteil (*Spoofing*).

Quelldatenreduktion zur Reduktion des Übertragungsvolumens ist vorteilhaft. Mit moderner Datenkompression benötigt man weniger als 6,4 kbit/s für die Sprachübertragung (anstatt 64 kbit/s wie vor dreissig Jahren) und überträgt zehn digitale Fernsehprogramme anstatt eines Analogprogramms.

Zu den Modulationsverfahren: Für analoge Verfahren gilt, je besser das Verhältnis von Hochfrequenzträgerleistung C zu Hochfrequenzrauschleistung N , desto besser die Qualität des Basisbandsignals in BER oder S relativ zur Rauschleistung R , also $S-R$.

Die technologisch fortschreitenden Modulationsverfahren liefern immer bessere Qualität – für eine entsprechende Leistung. Wenn die Leistung abfällt, fällt PSK die Bitfehlerrate entsprechend linear ab; die AM funktioniert ähnlich; mit $C-N < -10$ dB arbeitet sie immer noch, mit entsprechender Qualität.

Bei FM fällt die Qualität zunächst auch linear, bis ca. $C-N = 6$ dB, dann schwindet sie jedoch steil nach unten. Hochkomprimiertes Video mit MPEG verhält sich ähnlich wie FM.

Zum einen kann das Bild, wenn alle Bit korrekt sind, nicht mehr besser werden, und zum anderen bricht es ganz zusammen, wenn die Schwelle unterschritten wird. Man muss also die Übertragungsleistung sicherstellen. Dann ist MPEG vorteilhaft – weil es zehn Mal so viele Fernsehprogramme in einem Transponder abstrahlt, wie dies früher mit FM möglich war.

Die digitale Technologie ermöglicht heute auch, AM-Empfänger, die die Frequenz nachziehen, wenn sie driftet, und sonst ein paar Tricks anzuwenden, um Quaken und Quielen zu unterdrücken. Damit lassen sich Sprachkanäle in 2 kHz übertragen (*Single Sideband Frequency Compressed AM*; SSBFCAM). Diese Technik wurde aber weitgehend von der Digitaltechnik mit hochkomprimierten Sprach-

kanälen, die auch in 2 kHz übertragen werden können, „links überholt“; die SSBFCAM wurden in den USA Anfang der 90-er Jahre eingesetzt, haben sich aber nicht durchgesetzt.

Modulationsverfahren müssen der jeweiligen Übertragung angepasst werden. Die robusteste Digitalmodulation ist FSK (es ist technisch einfacher, eine von zwei bekannten Trägerfrequenzen zu detektieren als die unbekannte Phasenlage eines schwer detektierbaren Signals). FSK hat jedoch deutlich niedrigere Bandbreiteneffizienz.

PPM hat seinen Platz in der Funkortung, ist jedoch kein Vehikel für die Übertragung von grösseren Volumina von Daten.

Höhere Informationsvolumina werden am besten mit PSK übertragen. Hier kostet QPSK die gleiche Übertragungsleistung wie BPSK, benötigt aber nur die halbe Bandbreite. Deshalb sollte BPSK heute in der bandbreitenlimitierten Satellitenkommunikation nicht mehr eingesetzt werden.

Der Trend geht zu höherwertigen Phasenmodulationen, zu 8 PSK (mit 8 Phasenzuständen), 16PSK und 64QAM etc. Das 16QAM kostet etwa die gleiche Leistung wie 8PSK, benötigt jedoch nur ca. 2/3 der Bandbreite. Der nächste Schritt ist via 64QAM, das im Jahr 2000 (in München) via Satellit erfolgreich demonstriert wurde, und weiter zu 126QAM, 256QAM und 512QAM.

Kommunikationssatelliten sind längst nicht mehr leistungs- sondern bandbreitenbegrenzt. Mehrere Amplitudenzustände pro Phase fordern erhöhte Leistung, nicht aber erhöhte Bandbreite; deshalb geht man zu 64 QAM etc.

Literaturhinweise

- Mäusl, Rudolf, „*Digitale Modulationsverfahren*“, Hüthig, Heidelberg, 1995
- Proakis, John, „*Digital Communications*“, McGraw Hill, New York, 1995
- Berlin, Peter, „*The Geostationary Applications Satellites*“, Cambridge University Press, Cambridge, 1988
- Dixon, R. C., „*Spread Spectrum*“, Wiley-Interscience, New York 1994
- Fletscher, Walt, „*Voice Processing*“, Artech House, Boston, 1991
- Klaus Schmeh, „Kryptografie und Public-Key-Infrastrukturen im Internet“, dpunkt.verlag, 2001
- Beutelsbacher, A. und Wolfenstetter, K.-D.; „Sicherheit in IT-Systemen mit kryptographischen Methoden“; empfehlenswerter Lehrgang der CCG IT 6.14, Oberpfaffenhofen bei München, 2002
- R. Price and P.E. Green, „A communications technique for multipath channels“, US-Patent, 1956
- R. Price and P.E. Green, „A communications technique for multipath channels“, Proceedings of the IRE, Vol. 46, pp. 555-570, March 1958
- Feldhusen, J., „EDV-Technik“, Springer, 2006
- Hering, E., Martin, R., Stohrer, M., „Taschenbuch der Mathematik und Physik“, Springer, 2005
- Schuppen, J.H.v., „Mathematics of Control, Signals, Systems“, Springer, 2006