Fehlererkennung und -Korrektur

Kurzfassung u.a. für Prüfung (H. Völz, 9.2.07).

Im Gegensatz zur Kompression wird auf der Sendeseite *Redundanz hinzugefügt*. Sie ist systematisch so gestaltet, dass Störungen diese Struktur verändern und daher erkennbar bzw. korrigierbar sind. Wichtig sind vor allem Übertragungs- und Speicherverfahren, die mit fester Blocklänge arbeiten, auf die dann alles bezogen wird. Seltener sind kontinuierliche Verfahren (Übertragung von speziellen Streams, s.u.).

Wesentlich für die Analyse und Synthese sind die *Kanaleigenschaften*. Es werden *Ein-, Mehrbit- und Burstfehler* unterschieden. Sie sind statistisch vorhanden. Daher sind alle Aussagen statistisch. Burstfehler sind recht häufig: Ursachen sind Störstellen im Speichermedium, kurzzeitige Störsignale usw. Sie besitzen immer eine typische Länge.

*Einfache Erkennung*svarianten sind *Parity* und *Symmetrie*. Mit einer *Blockparity* auch Fehlerkorrektur für 1 Bit möglich.

Komplexe Verfahren benutzen spezielle *Algorithmen*. Dann sind Fehlererkennung und -korrektur gegeneinander abwägbar. Es werden 2^n *Signalwörter* von *n* Bit Länge und ihnen zugeordnete gültige *Kanalwörter* der Länge $m>n$ unterschieden. Dadurch gibt es $2^m - 2^n$ ungültige Wörter als *Redundanz*. Sie können durch Kanalstörungen auftreten und daher zumindest als solche erkennbar.

Der *Abstand* zwischen zwei beliebigen Wörtern ist durch die Anzahl der abweichenden Bit bestimmt. Zwischen allen gültigen Wörtern eines Codes gibt es einen minimalen Abstand, das ist der ***Hamming-Abstand.*** Je größer er ist, desto bessere Erkennungs- und Korrekturverfahren sind möglich.

Eine *anschauliche* Beschreibung ermöglichen 3-Bit-Wörter (Würfel). Für mehr Bit sind *aufwendige Verfahren* notwendig. Sie sind schwer zu finden und werden dann nach ihren Entwicklern benannt. Das wichtigste Prinzip beruht auf ***Polynome***, die dann gleichermaßen für Signale und Schaltungen (rückgekoppelte Schieberegister) gelten. Für Ihre Berechnung existiert die Galois-Theorie GF_n, vereinfacht kann sie durch eine *Modula-Arithmetik* zu *n* ersetzt werden. Besonders wichtig ist die binäre Arithmetik mit $n=2$ (digital). Es müssen die Addition, Subtraktion, Multiplikation und Division benutzt werden. Die Division ergibt oft einen Rest. Ähnlich wie für Primzahlen existieren *irreduzible Polynome* (auch *primitiv*). Sie sind ohne Rest nur durch 1 und sich selbst teilbar.

Rückgekoppelte Schieberegister-Ketten mit *l* Flipflops können unterschiedlich betrieben werden. Bei einer gegebenen Anfangsbelegung erzeugen sie (ohne zusätzliches Eingangssignal) mit dem Takt an den *l* Ausgängen eine periodische Signalfolge (Zyklus) der Länge *x*. Sie ist typisch für die Eingangsbelegung und die Schaltung (Polynom). Nur bei irreduziblen Polynomen werden alle möglichen Signalvarianten durchlaufen. Dieser Fall ist u.a. wichtig für *CRC, Randomizing und Zufallsgeneratoren*. In den anderen Fällen gibt es je nach Anfangsbelegung ausgewählte Signalfolgen. Sie sind u.a. die Basis für *gültige Code-Wörter*. Da in diesem Fall bei der Division eines ungültigen Code-Wortes ein Rest auftritt (*Syndrom*) kann damit die *Fehlererkennung und -korrektur* vorgenommen werden. Die Berechnung der einzelnen Verfahren ist sehr aufwendig und erfolgt durch hochspezialisierte Mathematiker, deren Namen dann die entstandenen Verfahren tragen. Es gibt kaum perfekte Code, die die *theoretischen Grenzen* (hierfür gibt es mehrere Abschätzungen) erreichen. Hierzu gehört u.a. der *Hamming-Code* in mehreren Varianten (Bitlängen und Hamming-Abständen). Ein erster och relativ einfaches Burstverfahren ist der *Fire-Code*.

Fehlerkorrektur erfolgt durch einzelne „Bit-Flips“. Hierzu müssen Orte in dem jeweiligen Block vorhanden sein. Einfach ist dies für 1-Bit-Fehler, kompliziert für viele Bit-Fehler. Daher ist **Burst-Korrektur** vorteilhaft. Dann braucht nach dem ersten Fehlerbit nur noch die gegebene Burst-Länge beachtet zu werden.

Äquivalent zur Polynom-Arithmetik ist das *Matrix-Verfahren*.

Neben den auf Datenblöcke bezogenen Codes gibt es auch fortlaufende. Sie sind u.a. als *Trellis-Codes* bekannt, werden z.T. aber auch bezüglich längerer Blöcke genutzt.

Empfohlene Literatur

Peterson, W. W.: Prüfbare und korrigierbare Codes. Oldenbourg - Verlag, München 1967 (alt aber sehr gut zur Einführung)

Friedrichs, B.: Kanalcodierung - Grundlagen und Anwendungen in modernen Kommunikationssystemen. Springer, Berlin - Heidelberg - New York, 1996. (sehr ausführlich)

Völz, H.: Wissen - Erkennen - Information. Allgemeine Grundlagen für Naturwissenschaft, Technik und Medizin. Shaker Verlag, Aachen 2001 (All Kapitel auf das Wesentliche beschränkt, auch auf meiner CD der digitalen Bibliothek vorhanden)