5 Codesicherung – Fehlererkennung und Fehlerkorrektur

Nachdem im vorhergehenden Kapitel viel über Zahlensysteme und Codierungen zu erfahren war, sollen nun verschiedene Möglichkeiten der Sicherung digitaler Daten gegen Übertragungsstörungen und sonstige Fehlerquellen vorgestellt werden.

5.1 Fehlerursachen und Störungen

Bei der Speicherung von Daten und Übertragung über beliebige Kommunikationskanäle, auf kurzen oder langen Wegen wie auf den öffentlichen Übertragungsnetzen, können Fehler auftreten. Dabei werden durch Störeinflüsse einzelne Bit oder auch ganze Bitgruppen verändert. Diese Störungen führen zur Verfälschung von einzelnen Symbolen als auch ganzen Nachrichten. Daher gibt es immer eine gewisse Wahrscheinlichkeit, dass ein am Empfänger eintreffendes Bitmuster nicht mit dem von der Datenquelle abgesandten übereinstimmt. So kann die Bitfehlerwahrscheinlichkeit bei der Übertragung auf Fernsprechleitungen bis zu $1 : 10^4$ betragen, d. h. im Mittel wird dann jedes 10.000. Bit falsch übertragen. Aufgabe einer Fehlersicherung ist es, die zu übertragenden Daten gegenüber Störeinflüssen zu sichern und Bitfehler in Codewörtern oder Codewort-Blöcken zu erkennen und/oder zu beseitigen. Das erfordert einerseits Maßnahmen zur Erkennung von Übertragungsfehlern und andererseits zu ihrer Korrektur zu ergreifen (Fehlerbehandlung). Zur Sicherung der übertragenen Daten verwendet man daher

- fehlererkennende Codes und/oder
- fehlerkorrigierende Codes (EDC – Error Detection and Correction).

Wie gezeigt wird, ist eine Fehlererkennung nur dann möglich, wenn durch Bitfehler ungültige Codeworte entstehen, also Codeworte, die nicht im vereinbarten Zeichenvorrat definiert sind. Bitfehler, die ein Codewort in ein anderes gültiges Codewort verfälschen, bleiben jedoch ohne entsprechende Maßnahmen unerkannt.

Störungen

„Fehler“ eines binären Signals bedeutet generell die Inversion, also Umkehrung dieses Signals: „0“ ⇒ „1“ und „1“ ⇒ „0“. Man bezeichnet dieses Bit dann als gekippt. Die verursachende Störung muss jedoch groß genug sein, um die physikalische Repräsentation der binären Pegel umzukehren. Je nach Repräsentation ist das nur schwer möglich, was wiederum ein großer Vorteil gegenüber der Analogtechnik ist. Die Intensität der Störung wird durch eine statistische Größe, die „Bitfehlerwahrscheinlichkeit“ ausgedrückt. Eine Bitfehlerwahrscheinlichkeit von z. B. 0,00001 ($= 10^{-5}$) bedeutet, dass von 100.000 korrekt übertragenen Bits im Mittel eines verfälscht wird. Die Bitfehlerwahrscheinlichkeit von 0 ist demnach eine theoretische Grenze, die jedoch mit endlichem Aufwand nicht erreichbar ist. Für ISDN-Leitungen der Deutschen Telekom AG wird z. B. eine Bitfehlerwahrschein-

lichkeit von 10^{-7} für sogenannte Dauerwählverbindungen (auch semipermanente Verbindung – SPV) angegeben.

Fehlerursachen

Die Signalstörungen auf Übertragungsstrecken für Digitaldaten können viele Ursachen haben. Die nachfolgende Zusammenstellung erhebt keinen Anspruch auf Vollständigkeit:

- Bandbreitenbeschränkung: Signalverzerrungen entstehen durch die begrenzte Bandbreite eines Kanals;
- Verzögerungsverzerrung: Die frequenzabhängigen Signallaufzeiten können bewirken, dass Oberwellen eines Signals während der Übertragung auseinander laufen und somit Signalverzerrungen bewirken;
- Rauschen wie elektronisches Rauschen oder das Impulsrauschen durch elektrische Geräte,
- thermische Elektronenbewegungen in Halbleitern oder Leitungen,
- Übersprechen oder Nebensprechen durch kapazitive oder induktive Kopplungen von anderen Leitungen bzw. benachbarten Datenkanälen,
- Einkopplungen durch Schaltvorgänge, insbesondere im Nahbereich von großen elektrischen Maschinen,
- Fehler, die durch Reflektion der Signale am Leitungsende entstehen,
- Kurzzeitstörungen wie elektrische Funken oder auch Kratzer auf CDs/DVDs,
- kosmische bzw. ionisierende Strahlung,
- Kombinationen aus mehreren unterschiedlichen Störungsursachen.

5.1.1 Fehlerarten

Man unterscheidet verschiedene Arten von Fehlern:

- Einzelbitfehler,
- Bündelfehler und
- Synchronisationsfehler.

Einzelbitfehler (*englisch:* single bit error) sind Fehler, die unabhängig von anderen Fehlern auftreten und allgemein für ein einzelnes verfälschtes Binärelement verantwortlich sind. Bei Bündelfehlern (auch Burst-Error, Block- oder Büschelfehler) handelt es sich um mehrere hintereinander auftretende fehlerhafte Bits, die, abhängig von anderen, während eines kurzen Abschnitts gehäuft auftreten und eine sehr ungleichmäßige Fehlerverteilung aufweisen. In der Telekommunikation tritt diese Art von Fehlerbündeln häufig durch Störeinflüsse wie Blitze, Übersprechen (crosstalk – unerwünschte gegenseitige Beeinflussung zwischen unabhängigen Signalkanälen), Relaisschaltungen usw. auf. Synchronisationsfehler sind meist längere Bündelfehler, die neben einem Verlust des Inhalts empfangener Symbole auch zu einem Verlust der Information darüber führen, wie viele Symbole

verloren gegangen sind. Das führt dazu, dass sich auch nachfolgende korrekt empfangene Symbole nicht mehr verwenden lassen, da nicht bekannt ist, an welche Stelle diese Symbole gehören.

Man kann das Speichern von Daten auf Speichermedien auch als eine Art Datenübertragung über einen längeren Zeitraum betrachten. Dabei entspricht das Senden der Daten dem Schreiben auf ein Speichermedium und das Empfangen dem Lesen. Dazwischen vergeht Zeit, in der das Speichermedium möglicherweise zerkratzt (CD, DVD) oder auf andere Art verändert werden kann. Beim Lesen der Daten aus den Speichern kann es somit zu Fehlern kommen.

Soft Errors

Ein Soft Error, oder zu deutsch „weicher" Fehler, auch als „Single Event Upset" (SEU) bezeichnet, kann in Halbleiterbausteinen beim Durchgang hochenergetischer ionisierender Teilchen (z. B. Schwerionen, Protonen, aber auch Alpha-Teilchen beim Alpha-Zerfall von Spuren schwerer Elemente wie Uran oder Thorium im Gehäusematerial) hervorgerufen werden. Beim Durchqueren gibt ein ionisierendes Teilchen Energie an das umliegende Halbleitermaterial ab, was zu einer Änderung der Ladungsverteilung bei einem p-n-Übergang führen kann. Ein SEU äußert sich dann beispielsweise als „Bitflip", ein Umkippen des Zustands eines Bits in Speicherbausteinen oder Registern, was zu einer Fehlfunktion nicht nur des betroffenen Bauteils, sondern kompletter Anlagen führen kann[2]. Die Klassifizierung als „Soft Error" rührt daher, dass ein SEU keinen dauerhaften Schaden am betroffenen Bauteil bewirkt. Da das Magnetfeld der Erde eine abschirmende Wirkung für hochenergetische Teilchen besitzt, treten SEUs in Meereshöhe nur relativ selten auf. Allerdings nimmt die Häufigkeit ihres Auftretens mit immer kleineren Halbleiterstrukturen zu, da mit kleiner Strukturgröße und höherer Taktfrequenz bereits geringere Energien ausreichen, um ein SEU zu provozieren. Große Bedeutung haben SEUs im Bereich der Luft- und Raumfahrt. Flugzeuge und vor allem Satelliten wie Raumfahrzeuge sind einer erhöhten (Teilchen-)Strahlung ausgesetzt, weshalb die Elektronik hier in höherem Maße betroffen ist.

5.1.2 Fehlerkorrektur

Auch für die Speicherung von Daten kann eine Fehlererkennung bzw. Fehlerkorrektur angebracht oder gar unerlässlich sein. Gespeicherte Daten werden daher mittels geeigneter Verfahren gegen Einzel- oder Mehrbitfehler gesichert, z. B. durch die „RS-Codierung" (Reed-Solomon-Codes, siehe entsprechenden Abschnitt). Im Falle eines SEUs, der die Änderung eines Speicherinhalts bewirkt, lassen sich so die korrekten Daten wiederherstellen. Wie bei der Datenübertragung ist auch hier abzuwägen, inwieweit eine Fehlerkorrektur nötig und vom Aufwand vertretbar ist. Für das Abspeichern einer längeren einfachen Textdatei braucht man meist keine Sicherheitsvorkehrungen zu treffen. Selbst wenn ein paar Bytes hintereinander falsch sind, so ist vielleicht nur ein Wort im Text unleserlich, was jedoch nicht viel ausmacht, da der Mensch meist selbst aus dem Satzzusammenhang

[2] Die Ausfallrate λ technischer Komponenten, insbesondere die elektronischer Bauteile, wird oft mit „Failure in Time" (Abk.: FIT) angegeben. Die Einheit FIT gibt dabei die Anzahl der Ausfälle an, die in 10^9 Stunden auftreten. 1 FIT ist somit 1 Ausfall pro 10^9 Stunden beziehungsweise 1 Ausfall pro 114.000 Jahre.

und der Redundanz der Sprache den Fehler korrigieren kann. Somit ist eine Textdatei ohnehin ausreichend redundant. Ganz anders verhält es sich beispielsweise bei einer gepackten ZIP-Datei. Tritt nur in einem einzigen Zeichen ein Fehler auf, so kann die Datei vollständig unbrauchbar werden, da die enthaltenen Informationen sehr dicht gepackt und somit nicht redundant sind. Daher nutzt das ZIP Format immer eine CRC-Prüfung (Cyclic Redundancy Code – siehe spätere Abschnitte), um wenigstens Fehler erkennen zu können. Weitere Beispiele sind ausführbare Dateien wie EXE-Dateien, „Binaries“ (Binärdateien ausführbarer Programme) etc. Wird hier nur ein Bit verändert, so kann dadurch das gesamte Programm bei der nächsten Ausführung „abstürzen“.

Warum Fehlererkennnung und -korrektur?

Wie eingangs festgestellt, sind Datenübertragungen häufig mit Fehlern behaftet. Enthält das jeweilige Übertragungsprotokoll keine Fehlererkennung, so merkt man erst nach einer eventuell längeren Übertragung, dass man noch mal von vorne beginnen muss. Gehört zu den Merkmalen des Protokolls neben der Fehlererkennung auch eine Fehlerkorrektur, so darf man sich trotz auftretender Fehler einer störungsfreien oder zumindest störungsarmen Übertragung relativ sicher sein. Das nachfolgende Bild 5.1 zeigt, ausgehend von einem abstrakten Schema der Nachrichten- bzw. Datenübertragung, einen Überblick zur Wirkungsweise von Fehlererkennung und -korrektur. Bei einer Nachrichtenübertragung mit Fehlerbehandlung muss man in der Decodierphase die durch Störungen entlang des Übertragungskanals entstandenen Fehler entdecken bzw. korrigieren können. Ein Fehler bedeutet generell, dass der Sender ein Codezeichen an den Kanal übergibt, beim Empfänger jedoch durch die Störung ein anderes Codezeichen ankommt.

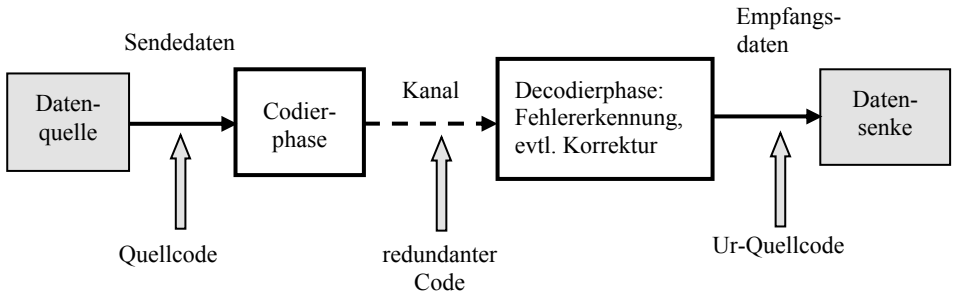

Bild 5.1: Prinzipielle Wirkungsweise von Fehlererkennung und -korrektur

Prüfdaten

Fehlererkennungs und -korrekturverfahren dienen somit dazu, Fehler bei der Speicherung und Übertragung von Daten zu erkennen und wenn möglich, auch zu korrigieren. Fehlererkennungsverfahren beschränken sich auf eine reine Fehlererkennung ohne Korrektur. Dazu wird vor der Datenspeicherung oder Übertragung den Nutzdaten Redundanz in Form zusätzlicher Bits hinzugefügt, die auf der Empfänger- bzw. Zielseite zur Bestimmung von Fehlern und ggf. deren Positionen genutzt wird. Man erkauft sich allerdings diese Fehlersicherheit zum Preis einer etwas längeren Datenübertragung als es bei einer immer fehlerfreien Leitung nötig ist, da neben den eigentlichen Nutzdaten auch Prüfdaten übertragen werden müssen. Es ist immer abzuwägen, in welchem Ausmaß eine Daten-

übertragung über einen bestimmten Kanal (sei es ein Modem, ein „SCSI“ = Small Computer System Interface etc.) einer Fehlererkennung bzw. Fehlerkorrektur bedarf oder ob zuviel Sicherheit wegen der längeren Übertragungszeiten durch zusätzliche (redundante) Prüfdaten zu einer unvertretbaren Leistungseinbuße führt.

5.1.3 Redundanz

Bei jeder Art von Fehlersicherung werden die Daten senderseitig durch Zusatzinformationen ergänzt, die empfangsseitig eine Feststellung oder sogar die Korrektur von Übertragungsfehlern ermöglichen. Diese Zusatzinformationen bezeichnet man als Redundanz oder redundante Bits. Unter dem Begriff Redundanz (*lateinisch:* redundare – überlaufen) versteht man allgemein in der Technik das zusätzliche bzw. mehrfache Vorhandensein funktional gleicher oder vergleichbarer Ressourcen eines technischen Systems (meist aus Sicherheitsgründen), die bei einem störungsfreien Normalbetrieb nicht benötigt werden. Derartige Ressourcen können z. B. Motoren, Baugruppen, Bauelemente, Teilsysteme, komplette Geräte, aber auch Steuerleitungen, Leistungsreserven oder Informationen sein. In aller Regel dienen diese zusätzlichen redundanten Ressourcen zur Erhöhung der Ausfall-, Funktions- bzw. Betriebssicherheit.

In der Informationstheorie gibt der Begriff der Redundanz an, wie viel Information im Mittel pro Zeichen in einer Informationsquelle mehrfach vorhanden ist. Eine Informationseinheit ist dann redundant, wenn sie ohne Informationsverlust weggelassen werden kann. Redundant ist somit der Teil einer Nachricht, der keine (Nutz-) Information enthält. In informations- und nachrichtentechnischen Anwendungen wird Redundanz gezielt eingesetzt, um Fehler zu erkennen oder gar zu korrigieren. Eine Erhöhung der Redundanz ermöglicht neben dem Erkennen von Fehlern auch zugleich deren Lokalisierung und damit deren Korrektur. Redundanz erlaubt somit eine Steigerung der Qualität (also weniger Fehler) auf Kosten der Quantität (nämlich einer höheren Datenrate). Das Ausmaß der jeweils einzusetzenden Redundanz richtet sich nach der für die jeweilige Anwendung geforderten Fehlertoleranz. Bei Bankgeschäften und in der Raumfahrt könnte ein einziges umgekipptes Bit viel Geld kosten oder große Schäden verursachen, während bei der Internet-Telefonie oder beim DVB (Digital Video Broadcasting) sogar der andauernde Verlust ganzer Datenpakete ohne wesentliche Bedeutung ist. Die Durchführung einer fehlertoleranten Kommunikation durch redundante Information gelingt deshalb, weil sich eventuell verloren gegangene oder verfälschte Teilinformationen vom Empfänger aus ihrem Kontext wieder rekonstruieren lassen. Ein Maß für die Fehlertoleranz ist die später zu erläuternde „Hamming-Distanz“.

Redundanz quantifiziert

Um den Begriff der Redundanz zu quantifizieren, kann man für sie folgende Beziehung einführen, nämlich als die relative zusätzliche Information, die zur Fehlererkennung verwendet wird, bezogen auf die eigentliche Nutzinformation:

$$\text{Redundanz} = \frac{\text{Anzahl der übertragenen Bits}}{\text{Anzahl der Nutzdatenbits}} - 1$$

Wäre die Zahl der übertragenen Bits gleich der Zahl der Nutzdatenbits, so ergibt sich für die Redundanz der Wert 1 – 1 = 0 → also keine Redundanz. Bei der nachfolgend beschriebenen Übertragung eines Bytes (= 8 Nutzdatenbits) mit einem zusätzlichen Paritätsbit lässt sich demnach für die Redundanz folgender Wert ermitteln:

Redundanz = 9/8 – 1 = 1,125 – 1 = 0,125

Fehler erkannt

Was kann man tun, nachdem ein Fehler erkannt wurde und keine Korrektur möglich ist? Hier gibt es mehrere Möglichkeiten. Zunächst kann nach Feststellung eines Fehlers eine Aufforderung zur Wiederholung der Nachricht seitens des Empfängers erfolgen, damit der Übertragungsvorgang wiederholt wird. Dieses Verfahren wird auch ARQ genannt (Automatic Repeat Request). Es ist bei weitem die am häufigsten angewendete Methode zur Fehlerbehandlung bei der Datenübertragung, da sie in vielen Bereichen ökonomischer ist, als der Aufwand für fehlerkorrigierende Verfahren. Beim ARQ-Verfahren werden korrekte bzw. falsche Blöcke durch eine Quittung des Empfängers „ACK“ (= Acknowledge) bzw. „NAK“ (Not Acknowledge) bestätigt. Sollte nach mehreren Wiederholungen der Fehler nicht behoben sein, so muss die Übertragung schließlich mit Ausgabe einer Fehlermeldung oder einer Fehlernachricht abgebrochen werden.

Korrektur

Bei fehlerkorrigierenden Verfahren wird die Redundanz so groß gewählt, dass bei wenigen Fehlern die korrekte Information aus den Empfangsdaten wieder rekonstruiert werden kann. Zwar lassen sich im Prinzip beliebig viele Fehler korrigieren, was aber nur mit sehr großer Redundanz möglich ist. Aus diesem Grunde werden solche Verfahren bei der Datenübertragung nur dann eingesetzt, wenn die Fehlerwahrscheinlichkeit sehr hoch ist, z. B. bei der drahtlosen Datenkommunikation mit Bluetooth. In weiteren Anwendungen wie bei der CD-Codierung sind die Methoden der Fehlerkorrektur sehr wichtig.

5.2 Zeichenweise Paritätssicherung

Heute verwendet man zur gesicherten Datenübertragung meist Fehlererkennungsverfahren, um beim Auftreten eines Fehlers durch geeignete Maßnahmen wie erneute Datenübertragung oder Abbruch unverfälschte Daten zu garantieren. Die meisten Verfahren berechnen zusätzliche Prüfinformation, welche durch Vergleich mit der entsprechenden Information beim Empfänger zur Fehlererkennung benutzt werden kann. Wichtig bei all diesen Verfahren ist, welche Klassen von Fehlern erkannt bzw. nicht erkannt werden und wie groß somit die Wahrscheinlichkeit ist, einen Fehler zu übersehen.

Codewörter

Übliche, recht einfache Methoden der Fehlersicherung arbeiten mit dem Hinzufügen von Paritätsbits. Nehmen wir an, wir wollen die Ziffern 0 bis 3 durch 2-Bit-Dualcodes übertragen:

0 → 00, 1 → 01, 2 → 10 und 3 → 11