m	Primitive Polynome $p(x)$	m	Primitive Polynome $p(x)$
1	$x+1$	9	x^9+x^4+1
2	x^2+x+1	10	$x^{10}+x^3+1$
3	x^3+x+1	11	$x^{11}+x^2+1$
4	x^4+x+1	12	$x^{12}+x^7+x^4+x^3+1$
5	x^5+x^2+1	13	$x^{13}+x^4+x^3+x+1$
6	x^6+x+1	14	$x^{14}+x^8+x^6+x+1$
7	x^7+x+1	15	$x^{15}+x+1$
8	$x^8+x^6+x^5+x^4+1$	16	$x^{16}+x^{12}+x^3+x+1$

Tabelle 2.1 Primitive Polynome

Eigenschaften von Schieberegistersequenzen

- Eine PN-Sequenz $\boldsymbol{c}$ der Länge 2^m-1 wird von einem Schieberegister der Länge m erzeugt, dessen Rückkopplungen einem primitiven Polynom entsprechen.
- Jede der 2^m-1 Initialisierungen (alle der 2^m Möglichkeiten außer lauter Nullen) erzeugen die 2^m-1 unterschiedlichen zyklisch verschobenen PN-Sequenzen $\boldsymbol{c}_k$.

In Tabelle 2.1 sind primitive Polynome bis zum Grad 16 angegeben, mit denen jeder mithilfe eines Rechners experimentieren kann. Man kann auch andere Polynome benutzen, wird jedoch feststellen, dass diese in der Regel eine PN-Sequenz mit kleinerer Periode $n < 2^m-1$ erzeugen.

2.3 Navigation

Die Navigation beruht auf zwei Komponenten: einer Landkarte und der Bestimmung der Position auf dieser Karte. In diesem Abschnitt wollen wir uns mit der technischen Realisierung der Positionsbestimmung beschäftigen. Beide Navigationssysteme, Galileo und GPS, benutzen hierzu das gleiche Konzept: Jeder Satellit sendet eine eigene Pseudo-Zufallsfolge periodisch zur Erde. Wie im letzten Abschnitt erläutert, ist eine Pseudo-Zufallsfolge eine durch eine Vorschrift berechenbare Folge der Länge n, deren Eigenschaften sehr ähnlich der einer Zufallsfolge sind.

Eine Pseudo-Zufallsfolge entsprechend Abschnitt 2.2.3 besteht aus Nullen und Einsen. Um diese abstrahlen zu können, ist es besser, die Null als +1 zu repräsentieren und die Eins als –1. Dann kann man im Fall einer Null die Schwingung $\sin(2\pi f\tau)$ abstrahlen und im Fall einer Eins die Schwingung $-\sin(2\pi f\tau)$, wobei f die Frequenz und τ die Zeit darstellt. Die Realisierung durch ±1 wird häufig in technischen Systemen verwendet: Man kann sich etwa eine elektrische Spannung von ±1 V vorstellen. Bei Addition von Spannungen oder elektromagnetischen Schwingungen gilt im Folgenden die normale Addition, d. h. $1+1=2$. Die Umwandlung der Null nach +1 und der Eins nach –1, wird für $c_i \in \{0,1\}$ durch die Abbildung

$(-1)^{c_i}$ realisiert. Für die folgenden Überlegungen brauchen wir keine elektromagnetischen Schwingungen zu betrachten, die Modellannahme ± 1 ist vollkommen ausreichend.

2.3.1 Satellitensequenzen

Wir wollen zunächst die Abbildung von binären Sequenzen mit 0 und 1 auf sog. antipodale Sequenzen mit 1 und –1 an einem Beispiel beschreiben.

Beispiel 2.25 Abbildung von $\{0, 1\}$ nach $\{1, -1\}$

Gegeben sei die Pseudo-Zufallsfolge $\boldsymbol{c} = 010\,0111$. Wir führen die Abbildung $x_i = (-1)^{c_i}$, $i = 0, 1, ...6$ durch, d. h. $x_i = 1$, wenn $c_i = 0$ ist, und entsprechend $x_i = -1$, wenn $c_i = 1$ ist. Damit erhalten wir

$$\boldsymbol{c} = (010\,0111) \quad \longrightarrow \quad \boldsymbol{x} = (1, -1, 1, 1, -1, -1, -1).$$

♢

Mit dieser Abbildung können wir die Korrelation und die Autokorrelation aus den Definitionen 2.19 und 2.22 anders schreiben. Sind $\boldsymbol{x}$ und $\boldsymbol{y}$ zwei Sequenzen, dann ist das Produkt $x_i \cdot y_i$ gleich 1, wenn beide Werte gleiches Vorzeichen haben, wenn also entweder $x_i \cdot y_i = 1 \cdot 1 = 1$, oder $x_i \cdot y_i = (-1) \cdot (-1) = 1$ ist. Das Produkt ist –1, wenn beide Werte unterschiedliches Vorzeichen aufweisen, also entweder $x_i \cdot y_i = -1 \cdot 1 = -1$ oder $x_i \cdot y_i = 1 \cdot -1 = -1$ gilt. Die Summe über die komponentenweisen Produkte ist genau die Anzahl der Übereinstimmungen minus der Anzahl der Nichtübereinstimmungen. Damit können wir die Korrelation berechnen durch

$$\Phi(\boldsymbol{x}, \boldsymbol{y}) = \frac{1}{n} \sum_{i=0}^{n-1} x_i \cdot y_i.$$

Beispiel 2.26 Korrelation antipodaler Sequenzen

Seien $\boldsymbol{x} = (1, -1, 1, 1, -1, -1, -1)$ und $\boldsymbol{y} = (-1, 1, -1, 1, -1, -1, 1)$ so ist die Korrelation

$$\Phi(\boldsymbol{x}, \boldsymbol{y}) = \frac{1}{7} \sum_{i=0}^{6} x_i \cdot y_i = \frac{1}{7}(-1 - 1 - 1 + 1 + 1 + 1 - 1) = -\frac{1}{7}.$$

♢

Damit ein Empfänger auf der Erde seine Position bestimmen kann, muss jeder Satellit seine Sequenz entsprechend **Bild 2.4** periodisch senden. Also sendet er die Folge

$$..., x_{n-2}, x_{n-1}, |x_0, x_1, ..., x_{n-1}, |x_0, ..., x_{n-1}, |x_0, x_1, ...$$

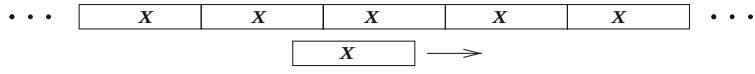

Bild 2.4 Autokorrelation durch Vorbeischieben

Beispiel 2.27 Periodische Sequenz

Die Sequenz des Satelliten ist $\boldsymbol{x} = (1, -1, 1, 1, -1, -1, -1)$. Dann sendet er

$$..., |1, -1, 1, 1, -1, -1, -1, |1, -1, 1, 1, -1, -1, -1, |1, -1, 1, 1, -1, -1, -1, |... .$$

♢

Schieben wir entsprechend Bild 2.4 die Sequenz $\boldsymbol{x}$ des Satelliten an der periodisch wiederholten Sequenz symbolweise vorbei und berechnen jeweils die Korrelation, so entspricht dies genau der Autokorrelation. Denn sieben aufeinanderfolgende Korrelationswerte sind genau alle sieben Werte der Autokorrelation. Wir wollen im Folgenden die Autokorrelation an einem Beispiel berechnen.

Beispiel 2.28 Autokorrelation der Sequenz des Satelliten

Zur Berechnung der Autokorrelation benutzen wir $\boldsymbol{x} = (1, -1, 1, 1, -1, -1, -1)$ und die um drei Stellen zyklisch verschobene Sequenz $\boldsymbol{x}_3 = (1, -1, -1, -1, 1, -1, 1)$ und summieren die komponentenweisen Produkte

$$\Phi(\boldsymbol{x}, \boldsymbol{x}_3) = \frac{1}{7}\sum_{i=0}^{6} x_i \cdot y_i = \frac{1}{7}(1 \cdot 1 + -1 \cdot -1 + 1 \cdot -1 + 1 \cdot -1 + -1 \cdot 1 + -1 \cdot -1 + -1 \cdot 1) = -\frac{1}{7}.$$

Entsprechend für die anderen zyklischen Verschiebungen:

$$\begin{aligned}
\boldsymbol{x} &= (1, -1, 1, 1, -1, -1, -1),\ \boldsymbol{x}_0 = (1, -1, 1, 1, -1, -1, -1), && \Phi(\boldsymbol{x}, \boldsymbol{x}_0) = 1\\
\boldsymbol{x} &= (1, -1, 1, 1, -1, -1, -1),\ \boldsymbol{x}_1 = (-1, 1, 1. - 1, -1, -1, 1), && \Phi(\boldsymbol{x}, \boldsymbol{x}_1) = -\frac{1}{7}\\
\boldsymbol{x} &= (1, -1, 1, 1, -1, -1, -1),\ \boldsymbol{x}_2 = (1, 1, -1, -1, -1, 1, -1), && \Phi(\boldsymbol{x}, \boldsymbol{x}_2) = -\frac{1}{7}\\
\boldsymbol{x} &= (1, -1, 1, 1, -1, -1, -1),\ \boldsymbol{x}_3 = (1, -1, -1, -1, 1, -1, 1), && \Phi(\boldsymbol{x}, \boldsymbol{x}_3) = -\frac{1}{7}\\
\boldsymbol{x} &= (1, -1, 1, 1, -1, -1, -1),\ \boldsymbol{x}_4 = (-1, -1, -1, 1, -1, 1, 1), && \Phi(\boldsymbol{x}, \boldsymbol{x}_4) = -\frac{1}{7}\\
\boldsymbol{x} &= (1, -1, 1, 1, -1, -1, -1),\ \boldsymbol{x}_5 = (-1, -1, 1, -1, 1, 1, -1), && \Phi(\boldsymbol{x}, \boldsymbol{x}_5) = -\frac{1}{7}\\
\boldsymbol{x} &= (1, -1, 1, 1, -1, -1, -1),\ \boldsymbol{x}_6 = (-1, 1, -1, 1, 1, -1, -1), && \Phi(\boldsymbol{x}, \boldsymbol{x}_6) = -\frac{1}{7}.
\end{aligned}$$

Die Autokorrelation nimmt also genau zwei Werte an, nämlich 1, wenn die Verschiebung 0 ist und $-\frac{1}{7}$ bei allen anderen Verschiebungen (< 7). ♢

Überlagerung von Satellitensequenzen

Der entscheidende Punkt für die Umsetzung der Positionsbestimmung ist, was passiert mit den Korrelationswerten, wenn sich zwei Zufallssequenzen überlagern? Seien $\boldsymbol{x}$ und $\boldsymbol{y}$ zwei Satellitensequenzen, dann ist $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}$ die überlagerte Sequenz, die gebildet wird, indem

für jedes $i = 0, 1, ..., n-1$, $z_i = x_i + y_i$ gesetzt wird. Folglich kann z_i die Werte $\{-2, 0, +2\}$ annehmen. Wir nutzen das Distributivgesetz, um die Korrelation von $\boldsymbol{x}$ mit $\boldsymbol{z}$ zu berechnen.

$$\Phi(\boldsymbol{x}, \boldsymbol{z}) = \frac{1}{n}\sum_{i=0}^{n-1} x_i z_i = \frac{1}{n}\sum_{i=0}^{n-1} x_i(x_i + y_i) = \frac{1}{n}\sum_{i=0}^{n-1} x_i x_i + \frac{1}{n}\sum_{i=0}^{n-1} x_i y_i = \Phi(\boldsymbol{x}, \boldsymbol{x}) + \Phi(\boldsymbol{x}, \boldsymbol{y}).$$

Da die Korrelation von $\boldsymbol{x}$ mit $\boldsymbol{y}$ erwartungsgemäß nahezu null ist (siehe Gl. (2.7) und Gl. (2.8)), ergibt die Korrelation von $\boldsymbol{x}$ mit $\boldsymbol{z}$ nahezu den gleichen Wert, wie die Korrelation von $\boldsymbol{x}$ mit $\boldsymbol{x}$. Entsprechendes gilt für die Korrelation von $\boldsymbol{y}$ mit $\boldsymbol{z}$.

$$\Phi(\boldsymbol{x}, \boldsymbol{z}) \approx \Phi(\boldsymbol{x}, \boldsymbol{x}) \text{ und } \Phi(\boldsymbol{y}, \boldsymbol{z}) \approx \Phi(\boldsymbol{y}, \boldsymbol{y}).$$

Beispiel 2.29 Überlagerung von Pseudo-Zufallssequenzen

Gegeben seien die Sequenzen $\boldsymbol{x}$ und $\boldsymbol{y}$, mit $\boldsymbol{x} = (1, -1, 1, 1, -1, -1, -1)$ und $\boldsymbol{y} = \boldsymbol{x}_2 = (1, 1, -1, -1, -1, 1, -1)$. Wir bilden die Summe von beiden

$$\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{x}_2 = \boldsymbol{x} + \boldsymbol{y} = (2, 0, 0, 0, -2, 0, -2)$$

und berechnen die Korrelation von $\boldsymbol{z}$ mit $\boldsymbol{x}$

$$\Phi(\boldsymbol{x}, \boldsymbol{z}) = \frac{1}{7}\sum_{i=0}^{6} x_i \cdot z_i = \frac{1}{7}\left(1 \cdot 2 + -1 \cdot 0 + 1 \cdot 0 + 1 \cdot 0 + -1 \cdot -2 + -1 \cdot 0 + -1 \cdot -2\right) = \frac{6}{7}.$$

Berechnen wir jedoch die Korrelation mit der Sequenz $\boldsymbol{x}_5$, so erhalten wir

$$\Phi(\boldsymbol{x}_5, \boldsymbol{z}) = \frac{1}{7}\left(-1 \cdot 2 + 1 \cdot -2 + -1 \cdot -2\right) = -\frac{2}{7}.$$

Der gleiche Wert ergibt sich für $\boldsymbol{x}_1$, $\boldsymbol{x}_3$, $\boldsymbol{x}_4$ und $\boldsymbol{x}_6$. Aber für $\boldsymbol{x}_2$ erhalten wir

$$\Phi(\boldsymbol{x}_2, \boldsymbol{z}) = \frac{1}{7}\left(1 \cdot 2 + -1 \cdot -2 + -1 \cdot -2\right) = \frac{6}{7}.$$

♢

Wir können damit Zufallsfolgen überlagern (addieren), und wenn wir mit der Folge korrelieren, die in der Überlagerung enthalten ist, erhalten wir einen Korrelationswert nahe 1. Korrelieren wir jedoch mit einer Folge, die nicht in der Überlagerung enthalten ist, erhalten wir eine Korrelation nahe 0.

Entsprechend Gl. (2.9) nimmt die Autokorrelation bei PN-Sequenzen die Werte $-\frac{1}{n}$ oder 1 an. Folglich steigt die Zuverlässigkeit der Korrelation mit der Länge n der Sequenz, weshalb Sequenzen der Länge 7 bzw. kurze Sequenzen für die praktische Anwendung nicht geeignet sind. Außerdem existieren bei kurzen Längen nicht genügend viele unterschiedliche Sequenzen, um jedem Satelliten eine eigene Sequenz zuzuweisen. Wir wollen an drei Satellitensequenzen ein Experiment durchführen, das in **Bild 2.5** skizziert ist. Drei unterschiedliche Pseudo-Zufallssequenzen $\boldsymbol{x}$, $\boldsymbol{y}$ und $\boldsymbol{z}$ der Länge 127 werden periodisch wiederholt

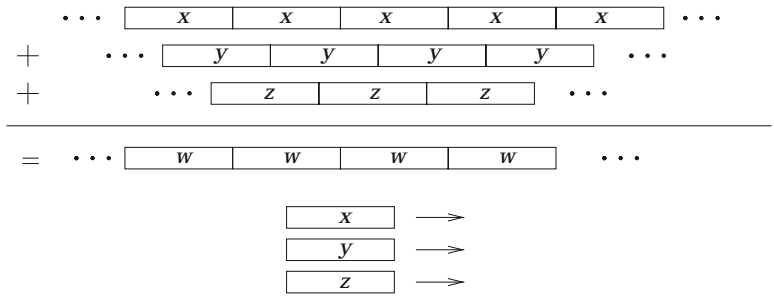

Bild 2.5 Überlagerung von drei Sequenzen

und addiert. Die zweite Folge y ist um 20 Stellen gegenüber x verschoben und die dritte um 60 Stellen. Die Summe der drei Sequenzen ist $z = x + y_{20} + z_{60}$. In Bild 2.5 ist durch die Pfeile angedeutet, dass x, y und z an z vorbeigeschoben werden und die Korrelation berechnet wird. Die Ergebnisse dieser Korrelationen sind in **Bild 2.6a** für x, in **Bild 2.6b** für y und in **Bild 2.6c** für z dargestellt. Man erkennt, dass beim Vorbeischieben und Korrelieren von x an z alle 127 Stellen ein deutliches Korrelationsmaximum vorliegt. Beim Korrelieren mit y ergeben sich ebenfalls deutliche Korrelationsmaxima, jedoch 20 Stellen später. Das gleiche gilt für z, 60 Stellen später. Wir können also festhalten, dass man die Differenz der Ankunftszeiten der Sequenzen eindeutig messen kann.

Das soeben beschriebene Experiment lässt sich auf noch mehr überlagerte Sequenzen und größere Sequenzlängen erweitern, sodass bei GPS und Galileo jeder Satellit seine individuelle Pseudo-Zufallssequenz abstrahlen kann. Bei GPS werden Sequenzen der Länge $n = 1\,023$ verwendet. Damit können die relativen Ankunftszeiten von den Sequenzen aller Satelliten, die empfangen werden können, aus der Überlagerung der Sequenzen berechnet werden. Selbstverständlich müssen die benutzten Satellitensequenzen dem Empfänger bekannt sein. Die Genauigkeit der Messung hängt natürlich von der zeitlichen Dauer eines Symbols ab. Wie man nun aus der Kenntnis der Differenz der Ankunftszeit die eigene Position berechnen kann, wollen wir im nächsten Abschnitt beschreiben.

2.3.2 Positionsbestimmung

Mit den bisherigen Ergebnissen sind wir in der Lage, die Differenz der Ankunftszeiten von zwei oder mehr Zufallssequenzen zu messen. Das Ergebnis der Messung gibt an, wie viel Symbole eine Sequenz später ankommt als die anderen Sequenzen. Mit den Differenzen der Ankunftszeiten wollen wir nun die Position bestimmen, an der sich ein Empfangsgerät befindet. Wir werden dazu schrittweise vorgehen und als erstes die eindimensionale Positionsbestimmung erläutern und anschließend die zwei- und dreidimensionale Positionsbestimmung beschreiben. Das Verfahren sollte bereits bei einer Dimension klar werden, die weiteren Dimensionen unterscheiden sich im Prinzip nur noch durch einen größeren Rechenaufwand.

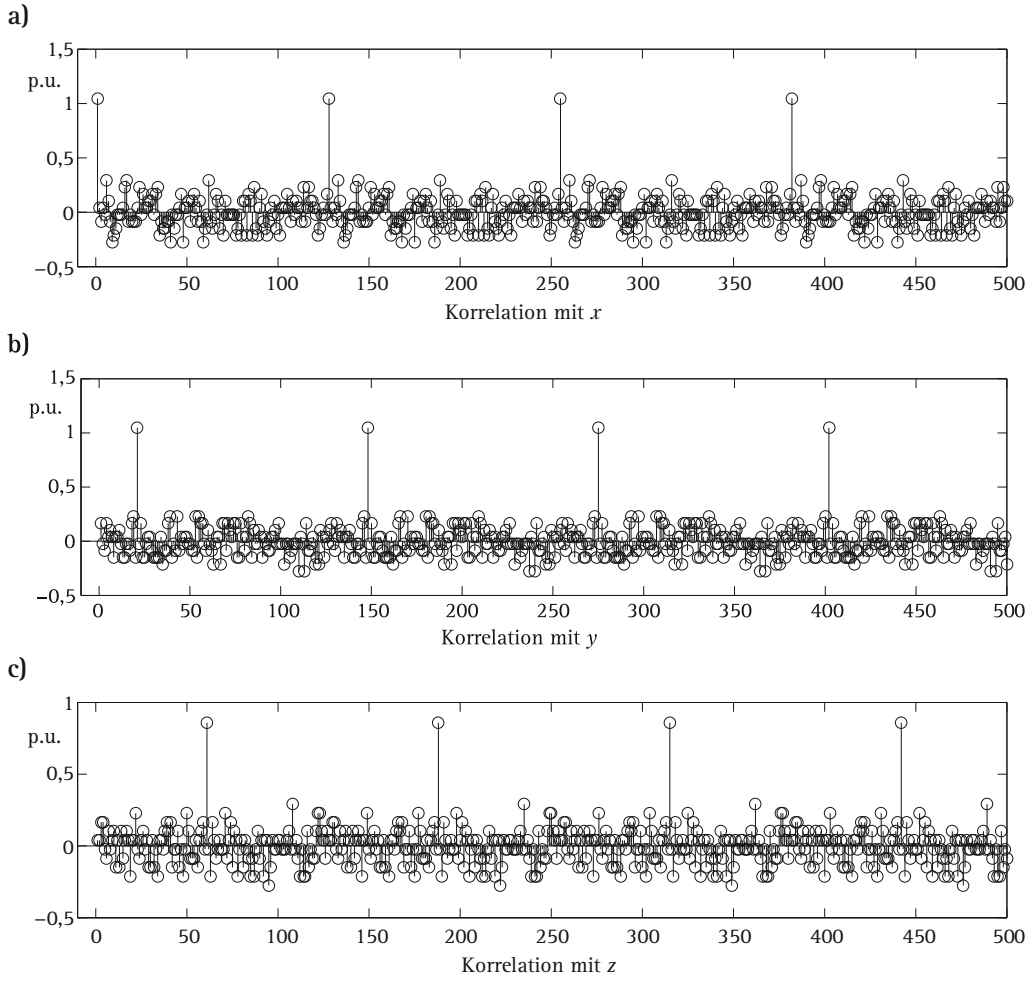

Bild 2.6 Korrelation der Summensequenz mit den einzelnen Sequenzen

Eindimensionale Positionsbestimmung

Wir wollen herausfinden wo wir uns auf einer Geraden befinden. Entsprechend **Bild 2.7** sind zwei Satelliten an den Stellen s_0 und s_1 positioniert. Wir befinden uns mit unserem Gerät an der Stelle s_n und empfangen die Überlagerung zweier Satellitensequenzen, die sich mit Lichtgeschwindigkeit ausbreiten. Wir nehmen an, dass beide Sequenzen zum gleichen Zeitpunkt τ_0 losgeschickt wurden und dass wir die Position s_0 und s_1 der Satelliten kennen. Durch Korrelation können wir, wie im vorherigen Abschnitt gezeigt, die relative Ankunftszeit, in Anzahl an Symbolen, berechnen. Wenn beide Sequenzen gleichzeitig ankommen, befinden wir uns in der Mitte von beiden Satelliten, d. h. an der Stelle $\frac{s_0+s_1}{2}$. Kommt das Si-

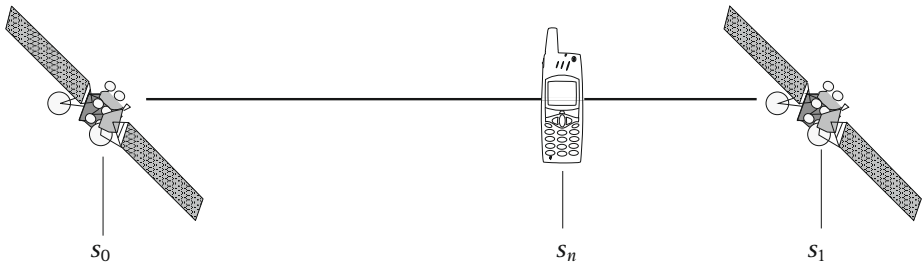

Bild 2.7 Eindimensionale Positionsbestimmung

gnal von s_0 vor dem von s_1 an, befinden wir uns links der Mitte und im anderen Fall rechts der Mitte. Wie nachfolgend gezeigt wird, entspricht die Strecke, die wir uns von der Mitte wegbefinden, genau der halben Laufzeitdifferenz mal der Lichtgeschwindigkeit. Um den Ort, an dem wir uns befinden, genau berechnen zu können, benötigen wir die Symboldauer.

Die in GPS verwendeten Satellitensequenzen sind aus der Familie der sog. Gold-Codes und haben, wie bereits erwähnt, eine Länge von 1 023 Symbolen. Die Rate mit der die Satellitensequenzen abgestrahlt werden, beträgt 1,023 Millionen Symbole pro Sekunde. Ein Symbol hat damit eine Dauer von $\frac{1}{1\,023\,000} = 9{,}775 \cdot 10^{-7}$ s und es dauert somit eine tausendstel Sekunde (eine Millisekunde, 1 ms), bis die komplette Satellitensequenz empfangen ist. Die Lichtgeschwindigkeit beträgt $c_0 \approx 2{,}997 \cdot 10^8 \frac{\text{m}}{\text{s}}$ was bedeutet, dass ein Symbol eine Länge von $2{,}997 \cdot 10^8 \cdot 9{,}775 \cdot 10^{-7} \approx 300\,\text{m}$ hat[1].

Sequenzlänge: $n = 1\,023$
Symboldauer: $T_c \approx 9{,}775 \cdot 10^{-7}$ s
Sequenzdauer: $T_s = 1$ ms
räumliche Symboldauer: $s_t \approx 300$ m
Lichtgeschwindigkeit: $c_0 \approx 2{,}997 \cdot 10^8 \frac{\text{m}}{\text{s}}$

Um die Position zu berechnen, nehmen wir zunächst an, dass das Signal des Satelliten bei s_0 zum Zeitpunkt t_0 und das vom anderen zum Zeitpunkt t_1 am Endgerät ankommt. Somit haben die Signale die Strecken $s_n - s_0$ und $s_1 - s_n$ in den Zeiten $t_0 - \tau_0$ bzw. $t_1 - \tau_0$ zurückgelegt. Mit der Lichtgeschwindigkeit c_0 und der Tatsache: Strecke ist gleich Geschwindigkeit mal Zeit, erhalten wir die beiden Gleichungen

$$s_n - s_0 = (t_0 - \tau_0) \cdot c_0,$$
$$s_1 - s_n = (t_1 - \tau_0) \cdot c_0.$$

[1] Da es hier nur um das Prinzip geht, wird darauf verzichtet, die vielen Nachkommastellen mitzuschleppen.

Zur Bestimmung von s_n subtrahieren wir zunächst diese beiden Gleichungen und lösen nach s_n auf

$$(s_n - s_0) - (s_1 - s_n) = (t_0 - \tau_0) \cdot c_0 - (t_1 - \tau_0) \cdot c_0,$$
$$s_n = \frac{s_0 + s_1}{2} + \frac{t_0 - t_1}{2} \cdot c_0. \tag{2.10}$$

Die Zeitdifferenz $(t_0 - t_1)$ ist dabei die Anzahl an Symbolen mal der Symboldauer $T_c \approx 9{,}775 \cdot 10^{-7}$. Der erste Summand in Gl. (2.10) berechnet die Mitte der beiden Satelliten und der zweite Summand berechnet die Entfernung nach links bzw. rechts von der Mitte, je nachdem, welches Satellitensignal als erstes ankommt. Damit ist die Position berechnet.

Da es zu aufwendig wäre, die Uhren der Endgeräte mit denen der Satelliten zu synchronisieren benutzt man, wie wir gesehen haben, eine Zeitdifferenzmessung und benötigt dazu zwei Satelliten, um die Positionsbestimmung in einer Dimension durchzuführen.

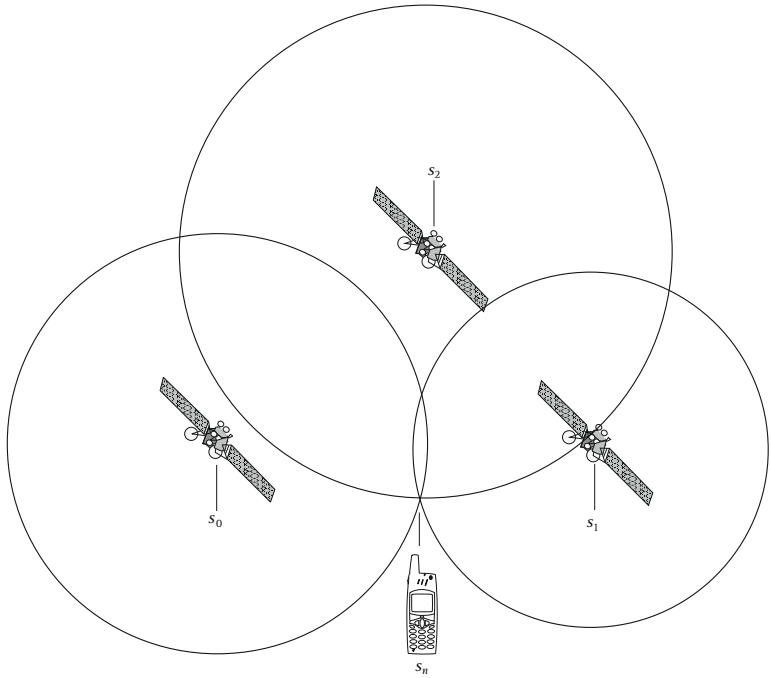

Bild 2.8 Zweidimensionale Positionsbestimmung

Zweidimensionale Positionsbestimmung

Wenn wir annehmen, dass wir uns auf einer Ebene befinden so müssen wir die zwei Koordinaten $s_n = (x_n, y_n)$ berechnen, an denen sich das Endgerät befindet. Empfangen wir

drei Satellitensignale, so sind uns zwei unterschiedliche Zeitdifferenzen bekannt. Entsprechend **Bild 2.8** befinden sich die Satelliten an den, als bekannt angenommenen, Koordinaten $s_0 = (x_0, y_0)$, $s_1 = (x_1, y_1)$ und $s_2 = (x_2, y_2)$. Die entsprechenden Ankunftszeiten der drei Signale seien t_0, t_1 und t_2. Wir können drei Gleichungen angeben

$$\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2} = (t_0 - \tau_0) \cdot c_0,$$
$$\sqrt{(x_n - x_1)^2 + (y_n - y_1)^2} = (t_1 - \tau_0) \cdot c_0,$$
$$\sqrt{(x_n - x_2)^2 + (y_n - y_2)^2} = (t_2 - \tau_0) \cdot c_0.$$

Aus diesen drei Gleichungen können wir durch Subtraktion zwei Gleichungen errechnen, in denen die zwei Unbekannten (x_n, y_n) vorkommen und zwei Zeitdifferenzen $(t_0 - t_1)$ und $(t_0 - t_2)$.

$$\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2} - \sqrt{(x_n - x_1)^2 + (y_n - y_1)^2} = (t_0 - t_1) \cdot c_0, \tag{2.11}$$
$$\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2} - \sqrt{(x_n - x_2)^2 + (y_n - y_2)^2} = (t_0 - t_2) \cdot c_0. \tag{2.12}$$

Aus diesen zwei Gleichungen kann man auf verschiedene Arten die zwei Unbekannten (x_n, y_n) berechnen. Wir wollen dies durch das sog. Newton-Verfahren tun. Dazu rufen wir uns zunächst den eindimensionalen Fall in Erinnerung. Gegeben sei eine Funktion $f(x)$. Die Tangente am Punkt x_0 lautet

$$y = f(x_0) + \frac{\mathrm{d}f(x_0)}{\mathrm{d}x}(x - x_0).$$

Durch null setzen dieser Tangente erhalten wir einen Schnittpunkt, der einen neuen Wert x_1 liefert. Damit können wir erneut eine Tangente

$$y = f(x_1) + \frac{\mathrm{d}f(x_1)}{\mathrm{d}x}(x - x_1)$$

berechnen. Dies wird fortgeführt, bis die Nullstelle der Funktion genügend genau erreicht wird.

Das gleiche Prinzip kann auf zwei Dimensionen erweitert werden. Beim zweidimensionalen Newton-Verfahren bildet man zunächst aus den Gl. (2.11) die zwei Funktionen $A(x_n, y_n)$ und $B(x_n, y_n)$.

$$A(x_n, y_n) = \sqrt{(x_n - x_0)^2 + (y_n - y_0)^2} - \sqrt{(x_n - x_1)^2 + (y_n - y_1)^2} - (t_0 - t_1) \cdot c_0 = 0,$$
$$B(x_n, y_n) = \sqrt{(x_n - x_0)^2 + (y_n - y_0)^2} - \sqrt{(x_n - x_2)^2 + (y_n - y_2)^2} - (t_0 - t_2) \cdot c_0 = 0.$$

Als nächstes benötigt man die Ableitung der beiden Funktionen. Da wir wegen der zwei Dimensionen zwei Variablen haben, bilden wir eine sog. partielle Ableitung nach x_n, bei der die Variable y_n einfach als Konstante betrachtet wird. Um eine partielle Ableitung von einer

Ableitung unterscheiden zu können, verwendet man statt d das Symbol ∂.

$$\frac{\partial A(x_n, y_n)}{\partial x_n} = \frac{x_n - x_0}{\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2}} - \frac{x_n - x_1}{\sqrt{(x_n - x_1)^2 + (y_n - y_1)^2}},$$
$$\frac{\partial B(x_n, y_n)}{\partial x_n} = \frac{x_n - x_0}{\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2}} - \frac{x_n - x_2}{\sqrt{(x_n - x_2)^2 + (y_n - y_2)^2}}.$$

Dann bilden wir die partielle Ableitung nach y_n

$$\frac{\partial A(x_n, y_n)}{\partial y_n} = \frac{y_n - y_0}{\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2}} - \frac{y_n - y_1}{\sqrt{(x_n - x_1)^2 + (y_n - y_1)^2}},$$
$$\frac{\partial B(x_n, y_n)}{\partial y_n} = \frac{y_n - y_0}{\sqrt{(x_n - x_0)^2 + (y_n - y_0)^2}} - \frac{y_n - y_2}{\sqrt{(x_n - x_2)^2 + (y_n - y_2)^2}}.$$

Seien u_0 und v_0 die ersten Schätzwerte für x_n und y_n, so lautet die Vorschrift für das Newton-Verfahren, eine Tangentialfläche z an eine Funktion f zu legen (was aus einer mathematischen Formelsammlung entnommen werden kann).

$$z = f(u_0, v_0) + \frac{\partial f}{\partial x_n}(u_0, v_0)(x_n - u_0) + \frac{\partial f}{\partial y_n}(u_0, v_0)(y_n - v_0).$$

Dies wenden wir auf unsere Funktionen $A(x_n, y_n)$ und $B(x_n, y_n)$ an und erhalten

$$z_A = A(u_0, v_0) + \frac{\partial A}{\partial x_n}(u_0, v_0)(x_n - u_0) + \frac{\partial A}{\partial y_n}(u_0, v_0)(y_n - v_0),$$
$$z_B = B(u_0, v_0) + \frac{\partial B}{\partial x_n}(u_0, v_0)(x_n - u_0) + \frac{\partial B}{\partial y_n}(u_0, v_0)(y_n - v_0).$$

Nun muss $z_A = z_B = 0$ gesetzt werden, was ein lineares Gleichungssystem ergibt, aus dem u_1 und v_1 berechnet werden können (u_0 und v_0 sind ja die bekannten Anfangswerte).

$$0 = A(u_0, v_0) + \frac{\partial A}{\partial x_n}(u_0, v_0)(u_1 - u_0) + \frac{\partial A}{\partial y_n}(u_0, v_0)(v_1 - v_0),$$
$$0 = B(u_0, v_0) + \frac{\partial B}{\partial x_n}(u_0, v_0)(u_1 - u_0) + \frac{\partial B}{\partial y_n}(u_0, v_0)(v_1 - v_0).$$

Jetzt sind u_1 und v_1 bekannt, und daraus kann man u_2 und v_2 berechnen, indem man erneut das lineare Gleichungssystem verwendet

$$0 = A(u_1, v_1) + \frac{\partial A}{\partial x_n}(u_1, v_1)(u_2 - u_1) + \frac{\partial A}{\partial y_n}(u_1, v_1)(v_2 - v_1),$$
$$0 = B(u_1, v_1) + \frac{\partial B}{\partial x_n}(u_1, v_1)(u_2 - u_1) + \frac{\partial B}{\partial y_n}(u_1, v_1)(v_2 - v_1).$$

Das wird solange durchgeführt, bis sich die Werte nicht mehr stark ändern, und man hat dann eine Schätzung der Position $\hat{x}_n = u_l$ und $\hat{y}_n = c_0$.

Bei der *dreidimensionalen Positionsbestimmung* benötigt man mindestens vier Satellitensignale. Das Newton-Verfahren kann dazu erweitert werden. Das Prinzip zur Berechnung der Position bleibt das gleiche, nur der Rechenaufwand steigt. In der Praxis werden natürlich alle verfügbaren Satellitensignale zur Positionsberechnung verwendet, was zu mehr Gleichungen führt, über deren Ergebnisse gemittelt werden kann. Ein sinnvoller Anfangswert kann dadurch bestimmt werden, dass man sich höchstwahrscheinlich irgendwo auf der Erde befindet.

2.4 Datenübertragung

Wie wir im vorherigen Abschnitt gesehen haben, muss die Position der Satelliten bekannt sein, da andernfalls die Positionsbestimmung nicht durchgeführt werden kann. Damit der Satellit seine Koordinaten in binärer Form dem Endgerät übermitteln kann, muss das folgende Problem gelöst werden: Wie kann man gleichzeitig mit den PN-Sequenzen, mit denen das Endgerät die Differenz der Ankunftszeiten misst, binäre Daten übertragen? Eine simple Idee wäre, wenn der Satellit eine 1 übertragen will, sendet er seine PN-Sequenz $\boldsymbol{x}$, und wenn er eine -1 übertragen will, sendet er $-\boldsymbol{x}$. Die Frage ist nur, was passiert bei der Korrelation im Endgerät? Kann man damit noch die Zeitdifferenz messen? Widmen wir uns zunächst einem Beispiel.

Beispiel 2.30 Datenübertragung mit PN-Sequenz

Sei die Sequenz des Satelliten $\boldsymbol{x} = (1, -1, 1, 1, -1, -1, -1)$. Der Satellit möchte die Daten ..., 1, −1, 1, ... übertragen, und sendet somit $..., \boldsymbol{x}, -\boldsymbol{x}, \boldsymbol{x}, ...$, also

$$..., \underbrace{1, -1, 1, 1, -1, -1, -1}_{\boldsymbol{x}}, \underbrace{-1, 1, -1, -1, 1, 1, 1}_{-\boldsymbol{x}}, \underbrace{1, -1, 1, 1, -1, -1, -1}_{\boldsymbol{x}}, ...$$

♢

Wir wissen, dass für die Korrelation von $\boldsymbol{z} = \boldsymbol{x} + \boldsymbol{y}$ mit $\boldsymbol{x}$ gilt:

$$\Phi(\boldsymbol{z}, \boldsymbol{x}) = \Phi(\boldsymbol{y}, \boldsymbol{x}) + \Phi(\boldsymbol{x}, \boldsymbol{x}) \approx \Phi(\boldsymbol{x}, \boldsymbol{x}),$$

da die Korrelation von unterschiedlichen PN-Sequenzen einen Wert nahe null ergibt. Die Korrelation von $\boldsymbol{x}$ mit $-\boldsymbol{x}$ hat den Wert

$$\Phi(\boldsymbol{x}, -\boldsymbol{x}) = \frac{1}{n}\sum_{i=0}^{n-1} x_i(-x_i) = \frac{1}{n}\sum_{i=0}^{n-1}(-1) = \frac{1}{n}(-n) = -1 = -\Phi(\boldsymbol{x}, \boldsymbol{x}).$$

Weiterhin ergibt die Korrelation von $\boldsymbol{y}$ mit $-\boldsymbol{x}$

$$\Phi(\boldsymbol{y}, -\boldsymbol{x}) = \frac{1}{n}\sum_{i=0}^{n-1} y_i(-x_i) = \frac{1}{n}\sum_{i=0}^{n-1}(-1)y_i x_i = (-1)\frac{1}{n}\sum_{i=0}^{n-1} y_i x_i = -\Phi(\boldsymbol{y}, \boldsymbol{x}),$$

wobei wir ausgenutzt haben, dass man einen konstanten Faktor vor die Summe schreiben kann. Damit erhalten wir für die Korrelation von z mit x, wenn $z = y + (-x)$ ist

$$\Phi(z, x) = \Phi(y, -x) + \Phi(-x, x) \approx -\Phi(x, x).$$

Wir haben damit gezeigt, dass bei Verwendung von invertierten Sequenzen das Korrelationsmaximum in ein Korrelationsminimum mit gleichem Betrag übergeht. In Bild 2.5 sind dann bei jedem Satelliten, entsprechend der Daten die er senden will, die Sequenzen $-x$ oder x, $-y$ oder y und $-z$ oder z enthalten. Die Korrelation mit x, y oder z liefert dann Korrelationsmaxima oder -minima an den Stellen, an denen die Sequenz enthalten ist. Es ergibt sich eine entsprechende Grafik, wie in den Bildern 2.6a bis 2.6c dargestellt, mit den betragsmäßigen Korrelationsmaxima an den gleichen Stellen, jedoch mit dem Unterschied, dass sie nach oben und unten zeigen können, je nachdem, welches Symbol gesendet wurde. Man kann also immer noch genau die Differenz der Ankunftszeit zu anderen Sequenzen bestimmen und gleichzeitig binäre Symbole $\{1, -1\}$ übertragen.

Da eine Sequenz eine Millisekunde $\left(\frac{1}{1\,000}\ s\right)$ dauert, kann man damit 1 000 Informationsbit pro Sekunde vom Satelliten an das Endgerät übertragen. Darin enthalten sind die Position des Satelliten, eine Zeitreferenz und weitere Informationen zum System.

2.5 Verschlüsselung

Nur wer eine Genehmigung hat ein System zu nutzen, erhält einen Schlüssel dafür. In den Anfängen war GPS verschlüsselt, und nur wer einen Schlüssel besaß, konnte das System in voller Genauigkeit nutzen. Die Sequenzen wurden bewusst gestört und nur die Teilnehmer mit Schlüssel konnten diese Störung herausrechnen. Im Mai des Jahrs 2000 wurde diese Störung abgeschaltet, was die uneingeschränkte Nutzung für alle ermöglichte. Der Effekt der Störung war, dass die momentane Position zufällig um bis zu 100 m verfälscht wurde. Wenn der Empfänger an einer Stelle stand, hat er sich gemäß den Messwerten zufällig in einem Gebiet von 100 m Radius bewegt. Damit war das System für viele Anwendungen unbrauchbar.

Wir können darüber spekulieren, was die US-Regierung dazu bewogen hat, die Störung und die Aussendung der verschlüsselten Information abzuschalten. Vielleicht war dies den cleveren Ingenieuren zu verdanken, die folgendes System installieren wollten. Man stellt an einen festen Punkt, dessen Koordinaten bekannt sind, ein GPS-Gerät auf und misst den Ort gemäß gestörtem GPS. Da der Ort des Geräts genau bekannt ist, kann so der Fehler gemessen werden. Diesen Fehler überträgt man sofort per Rundfunk an alle GPS-Nutzer, die damit ihre Messung korrigieren können. Somit wäre die bewusste Störung korrigierbar und damit unwirksam. Dieser Trick ist unter dem Namen differenzielles GPS bekannt. Doch wenden wir uns lieber den Methoden der Verschlüsselung zu.

Julius Cäsar, *Blaise de Vigenère* und *Gilbert Vernam*

Die Verschlüsselung von Text ist sehr alt. Bereits *Julius Cäsar* (13.7.100 – 15.3.44 v. Chr.) hat eine Verschlüsselungsmethode benutzt, die wie folgt funktioniert. Jeder Buchstabe eines

Worts wird durch den um drei Stellen späteren Buchstaben des Alphabets ersetzt. Diese Verschlüsselungsmethode ist zyklisch, d. h., statt z wird c geschrieben. Ein Beispiel zeigt die Verschlüsselung seines berühmten Satzes.

Beispiel 2.31 Cäsar-Verschlüsselung

Für diejenigen, die kein Latein gelernt haben, ist der Klartext bereits verschlüsselt. Veni, vidi, vici lautet übersetzt: Ich kam, sah und siegte. Wir schieben zur Verschlüsselung dieses Texts jeden Buchstaben um drei Buchstaben im Alphabet weiter. Beispielsweise wird dann I zu L.

$$\text{VENI, VIDI, VICI.} \quad \longrightarrow \quad \text{YHQL, YLGL, YLFL.}$$

♢

Diese Methode war natürlich nicht sehr sicher und sehr einfach zu knacken. Viel später, im Jahr 1586, hat der französische Diplomat *Blaise de Vigenère* die Methode *Julius Cäsar* verbessert, indem er einen Schlüssel aus Buchstaben eingeführt hat. Man verwendet zur Verschlüsselung nicht den um drei Stellen späteren Buchstaben, sondern den um so viele Buchstaben späteren, wie der Buchstabe des Schlüssels im Alphabet darstellt. Mit dem Schlüssel HEUTE wird mit dieser Verschlüsselungsmethode der erste Buchstabe des Klartexts durch den im Alphabet um acht Stellen spätere ersetzt, da H der achte Buchstabe des Alphabets ist, der zweite durch den um fünf Stellen späteren, da E der fünfte Buchstabe ist, der dritte um 21 Stellen wegen U, der vierte um 20 Stellen wegen T, und der fünfte erneut um fünf Stellen wegen E. Danach wird das ganze periodisch wiederholt.

Beispiel 2.32 Vigenère-Verschlüsselung

Mit dem Schlüssel HEUTE wollen wir nun *Julius Cäsars* berühmtes Zitat „VENI, VIDI, VICI“ verschlüsseln. Wir erhalten

$$\text{VENI, VIDI, VICI.} \quad \longrightarrow \quad \text{DJIC, AQID, PNKN.}$$

Der verwendete Schlüssel lautet HEUTEHEUTEHE, und man erkennt, dass er sich periodisch wiederholt. ♢

Wegen seiner Periode konnte dieses Verfahren ebenfalls geknackt werden, und zwar im Jahr 1863 durch *Friedrich Wilhelm Kasiski*, einen preußischen Major. Dieser hat zunächst aufgrund der unterschiedlichen Häufigkeit der einzelnen Buchstaben des Alphabets[1] die Periodenlänge des Schlüssels herausgefunden. Und dann, ebenfalls durch die Häufigkeiten, den Schlüssel selbst, was verhältnismäßig einfach ist. Denn wurde ein deutscher Text mit dem Verfahren von *Julius Cäsar* verschlüsselt, ist der häufigste Buchstabe das H, da er dem verschlüsselten E entspricht. Ist also der häufigste Buchstabe das H, so ist der entsprechende Schlüsselbuchstabe ein C. Ist der häufigste Buchstabe dagegen ein L, so ist der entsprechende

[1] Die Wahrscheinlichkeit für „e“ in einem deutschen Text ist 0,17 und für „j“ 0,0 027; die Leerzeichen eines Texts sind dabei nicht berücksichtigt.

Schlüsselbuchstabe ein G. Kennt man also die Periodenlängen des Schlüssels, so kann das Verfahren leicht geknackt werden.

Von *Gilbert Vernam* aus dem Jahr 1926 stammt die Methode, den Schlüssel bei der Vigenère-Verschlüsselung genau so lang wie den zu verschlüsselnden Text zu machen. Dies wird auch als One-Time-Pad bezeichnet und weist die bestmögliche Sicherheit auf. Kein Mithörer kann die Verschlüsselung knacken. Dieses Prinzip machte sich die Verschlüsselungsmaschine Enigma, die im Zweiten Weltkrieg benutzt wurde, zu eigen, indem sie pseudozufällige Sequenzen erzeugt hat. Enigma wurde letztlich auch geknackt, weil es eben nur pseudozufällige Sequenzen waren.

Beispiel 2.33 Vernam-Verschlüsselung

Da der zu verschlüsselnde Klartext „VENI, VIDI, VICI." aus zwölf Buchstaben besteht, benötigen wir einen Schlüssel, der aus mindestens zwölf Buchstaben besteht. Wir verwenden den Schlüssel FOTOSATELLIT. Damit ergibt sich:

$$\text{VENI, VIDI, VICI.} \quad \longrightarrow \quad \text{BTHX, OJXN, HULC.}$$

♢

Stromverschlüsselung

Heute verwendet man statt Buchstaben binäre PN-Sequenzen, die in Abschnitt 2.2.3 beschrieben wurden. Diese Methode wird als Stromverschlüsselung bezeichnet und ist in **Bild 2.9** dargestellt. Dabei wird zur Verschlüsselung die Nachricht $\boldsymbol{c}$ komponentenweise mit der PN-Sequenz $\boldsymbol{n}$ binär addiert, also $0 + 0 = 1 + 1 = 0$ und $1 + 0 = 0 + 1 = 1$ für alle Stellen c_i und n_i gebildet. Es wird dann $a_i = c_i + n_i$ gesendet. Die Entschlüsselung erfolgt beim Empfänger ebenfalls durch Addition von n_i zu a_i. Dabei ergibt sich in der Tat wieder c_i, da $n_i + n_i = 0$ ist, unabhängig davon, ob der Wert von n_i null oder eins ist.

Der Schlüssel, der ausgetauscht werden muss, ist die Initialisierung der Speicher des Schieberegisters. Starten Sender und Empfänger das Schieberegister mit der gleichen Initialisierung, so können sie die identische PN-Sequenz $\boldsymbol{n}$ erzeugen.

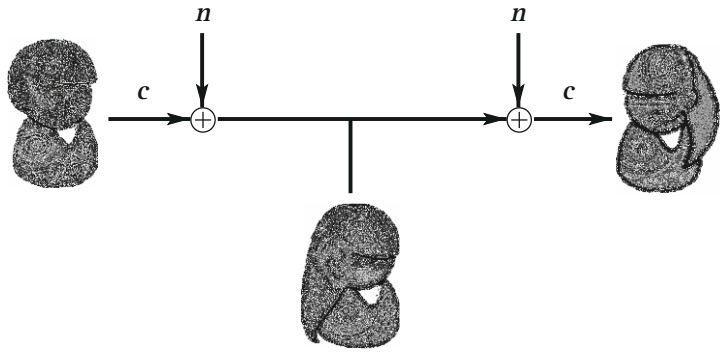

Bild 2.9 Stromverschlüsselung mit binären PN-Sequenzen

In der Praxis verwendet man die PN-Sequenzen, die durch Schieberegister erzeugt werden, nicht direkt, sondern verwendet mehrere Schieberegister, die man nicht linear verknüpft. Auf diesen Aspekt der Nichtlinearität kann hier nicht näher eingegangen werden: Er bewirkt jedoch, dass die Verschlüsselung schwieriger zu knacken ist. Die in GPS verwendete PN-Sequenz wird durch vier primitive Polynome vom Grad 12 erzeugt. Die PN-Sequenz entsteht durch nicht lineare Verknüpfung dieser vier Schieberegister. Die vier Schieberegister mit jeweils zwölf Speicherplätzen haben damit insgesamt 48 binäre Speicherplätze, was bedeutet, es existieren $2^{4 \cdot 12} = 2^{48} \approx 2{,}8 \cdot 10^{14}$ unterschiedliche Schlüssel. Nur wenn man den Schlüssel kennt, kann man die PN-Sequenz $\boldsymbol{n}$ aus Bild 2.9 erzeugen und so die Daten $\boldsymbol{c}$ berechnen. Die Daten werden mit 1 000 bit/s abgestrahlt, d. h., es dauert $2{,}8 \cdot 10^{11}$ s, bis eine Periode der PN-Sequenz gesendet ist. Dies entspricht etwa 9 000 Jahren.

Die Stromverfahren, die aktuell standardisiert werden, bestehen aus Schieberegistern mit insgesamt 128 Speichern. Es existieren also $2^{128} \approx 3{,}4 \cdot 10^{38}$ verschiedene Schlüssel und, wie wir oben gesehen haben, entspricht diese Zahl auch der Periode der Sequenz. Im Vergleich dazu enthält unser gesamtes Universum etwa 2^{263} Protonen. Selbst wenn man diese Sequenz mit einem Gigabit (10^9) pro Sekunde überträgt, benötigt man dazu ca. 10^{22} Jahre. Übrigens ist das Alter unseres Universums $13{,}7 \cdot 10^9$ Jahre.