Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 70 (1979)

Heft: 11

Artikel: Der binäre Golay-Code

Autor: Fabijanski, J.

DOI: https://doi.org/10.5169/seals-905385

Der binäre Golay-Code

Von J. Fabijanski

681.3.04:519.711.4;

Die wichtigsten Eigenschaften des dichtgepackten und des erweiterten Golay-Codes werden dargelegt. Anschliessend werden die Gewichts- bzw. Distanzverteilungen sowie explizite Ausdrücke für die Wahrscheinlichkeit des richtigen Empfanges und des Fehlempfanges abgeleitet.

L'article comporte un exposé des qualités fondamentales du code binaire de Golay, tant parfait qu'élargi. On en déduit ensuite les répartitions du poids et de la distance ainsi que les formules explicites pour la probabilité de la réception correcte et intempestive.

1. Einleitung

Für die Übertragung von Informationen werden meistens binäre Blockcodes verwendet [1; 2; 3]. Ein solcher Code bildet eine Menge von Codeworten, die n binäre Elemente (Bits) enthalten. Von diesen gelten üblicherweise die ersten k als Informationselemente und die restlichen $r = n - k$ als redundante Paritätselemente, die es ermöglichen, Bitfehler innerhalb des Codewortes zu erkennen bzw. zu korrigieren.

Der Code wird demnach durch das geordnete Tripel (n, k, d) charakterisiert, wobei d die minimale Hamming-Distanz zwischen den Codeworten bedeutet. Die Hamming-Distanz ist bekanntlich als die Anzahl der Binärstellen definiert, an denen sich zwei Codeworte voneinander unterscheiden.

Die Codeworte, als Folgen von Nullen und Einsen, können als Vektoren aufgefasst werden. Mit der elementenweisen Addition modulo 2 (die in diesem Fall mit der Subtraktion identisch ist) und Multiplikation mit 0 und 1 bilden sie über dem Galois-Körper $GF(2)$ eine additive abelsche Gruppe und einen k-dimensionalen linearen Unterraum des n-dimensionalen Vektorraumes aller möglichen Worte der Länge n. Solche Codes werden daher als *lineare* Codes bzw. *Gruppencodes* bezeichnet.

Die Codeworte (einschliesslich des Codewortes aus lauter Nullen, das normalerweise nicht benutzt wird) müssen in ihrem Informationsteil unterschiedlich sein, ihre Anzahl ist also der Anzahl der k-Variationen von 2 Elementen, d. h. 2^k gleich. Sie bilden folglich eine Teilmenge der Menge aller möglichen Worte der Länge n, deren Anzahl 2^n ist.

Die r Paritätselemente werden so gewählt, dass zum Code nur diejenigen Vektoren gehören, die die Bedingung $\boldsymbol{H}\boldsymbol{c}^{\mathrm{T}} = 0$ erfüllen. Dabei ist $\boldsymbol{H}$ eine Matrix mit Elementen aus $GF(2)$ und c^{T} der transponierte Codevektor, also ein Spaltenvektor mit n Elementen. Die dem Code eigene Paritätsmatrix $\boldsymbol{H}$ hat r Zeilen und n Spalten. Sie besteht aus einer rechteckigen Matrix $\boldsymbol{A}$ mit k Spalten und einer Einheitsmatrix $\boldsymbol{I}_r$ vom Grad r: $\boldsymbol{H} = [\boldsymbol{A}, \boldsymbol{I}_r]$.

Diese Bedingung definiert den Code eindeutig. Sie bildet auch die Grundlage für die selbsttätige Korrektur der Bitfehler im empfangenen Wort. Wenn nämlich das gesendete Codewort fehlerlos empfangen wird, so ist diese Bedingung offenbar erfüllt. Wenn aber das obige Produkt vom Nullvektor verschieden ist, so enthält es (als das sog. Syndrom) die Information über die Stellen, an welchen Bitfehler aufgetreten sind, vorausgesetzt, dass diese die für den Code zulässige Höchstzahl e nicht übersteigen. Die Fehler können dann rückgängig gemacht und das gesendete Codewort kann erkannt werden.

Wenn man sich die Endpunkte aller Codevektoren als Mittelpunkte von Kugeln mit dem Radius e (im Sinne der Hammingschen Metrik) im n-dimensionalen Raum denkt, so muss die minimale Distanz zwischen den Codeworten zumindest

$$d = 2e + 1 \tag{1}$$

betragen, damit diese Kugeln disjunkt und somit die mit höchstens e Bitfehlern behafteten Codeworte eindeutig identifizierbar sind.

Unter den linearen Codes gibt es eine besondere Klasse der sog. *perfekten* oder *dichtgepackten* Codes. Derartige Codes (sofern sie existieren) erlauben es, mit der minimalen Hamming-Distanz nach (1) bis zu e Bitfehlern innerhalb des Codewortes (aber keine mehr) zu korrigieren. Sie sind «dichtgepackt» in dem Sinne, dass die 2^k n-dimensionalen Kugeln um die Codeworte den gesamten Vektorraum restlos ausfüllen, und zwar derart, dass jeder Vektor zu nur einer Kugel gehört und dass es keine gibt, die zu keiner Kugel gehören. Die notwendige Bedingung für eine solche Zerlegung des Vektorraumes ist

$$\sum_{i=0}^{e} \binom{n}{i} = 2^{n-k} \tag{2}$$

Die Anzahl der jeder Kugel zugehörigen Vektoren ist nämlich gleich der Summe der Zahlen $\binom{n}{i}$ der i-Kombinationen von n Elementen für $i = 0, ..., e$. Diese Anzahl, multipliziert mit der Anzahl 2^k der Kugeln, muss die Anzahl 2^n aller Vektoren des Raumes ergeben, woraus die obige Bedingung unmittelbar folgt.

Es gibt freilich verhältnismässig wenige ganzzahlige Wertetripel (n, k, d), die (2) mit (1) erfüllen. Für diejenigen allerdings, die dies erfüllen, ist auch die Bedingung (2) nicht hinreichend für die Existenz eines entsprechenden Codes. Es muss in jedem Fall zusätzlich nachgewiesen werden, dass der betreffende Code tatsächlich existiert, d. h. nicht in sich widersprüchlich ist.

2. Die dichtgepackten Codes

Ein triviales Beispiel des dichtgepackten Codes ist der sog. Wiederholungscode, in dem ein Informationsbit einfach mehrmals wiederholt wird. Er enthält nur zwei Codeworte, bestehend aus lauter Nullen (das Nullwort) oder aus lauter Einsen (das Einswort). Mit e korrigierbaren Bitfehlern ist hier $(n, k, d) = (2e + 1, 1, 2e + 1)$, was die Bedingung (2) erfüllt, denn

$$\sum_{i=0}^{e} \binom{2e+1}{i} = 2^{2e}$$

Ein praktisch viel wichtigeres Beispiel bilden die Hamming-Codes $(2^r - 1, 2^r - 1 - r, 3)$, die freilich nur einen Bitfehler zu korrigieren vermögen [2; 3]. Hier hat man nämlich

$$\sum_{i=0}^{1} \binom{2^r - 1}{i} = 2^r.$$

Nach zahlreichen Versuchen hat *Golay*[1]) im Jahre 1949 [4] für binäre Codes noch zwei Wertetripel (n, k, d) gefunden, die die Bedingung (2) erfüllen, und zwar: (90, 78, 5) und (23, 12, 7). Er hat aber gleichzeitig festgestellt [4; 5], dass es für das erste Wertetripel keinen widerspruchslosen Code geben kann. Für das zweite hingegen hat er ein konkretes Beispiel eines linearen Codes (23, 12, 7) angegeben, definiert durch die Paritätsmatrix:

$$\boldsymbol{H} = \left[\begin{array}{cccccccccccc|ccccccccccc} 1&0&0&1&1&1&0&0&0&1&1&1 & 1&0&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&0&1&1&0&1&1&0&0&1 & 0&1&0&0&0&0&0&0&0&0&0&0 \\ 1&0&1&1&0&1&1&0&1&0&1&0 & 0&0&1&0&0&0&0&0&0&0&0&0 \\ 1&0&1&1&1&0&1&1&0&1&0&0 & 0&0&0&1&0&0&0&0&0&0&0&0 \\ 1&1&0&0&1&1&1&0&1&1&0&0 & 0&0&0&0&1&0&0&0&0&0&0&0 \\ 1&1&0&1&0&1&1&1&0&0&0&1 & 0&0&0&0&0&1&0&0&0&0&0&0 \\ 1&1&0&1&1&0&0&1&1&0&1&0 & 0&0&0&0&0&0&1&0&0&0&0&0 \\ 1&1&1&0&0&1&0&1&0&1&1&0 & 0&0&0&0&0&0&0&1&0&0&0&0 \\ 1&1&1&0&1&0&1&0&0&0&1&1 & 0&0&0&0&0&0&0&0&1&0&0&0 \\ 1&1&1&1&0&0&0&0&1&1&0&1 & 0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&1&1&1&1&1&1&1&1&1&1&1 & 0&0&0&0&0&0&0&0&0&0&1&0 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&0 & 1&0&0&0&0&0&0&0&0&0&0&1 \end{array}\right] \quad (3)$$

Der durch diese Matrix $\boldsymbol{H}$ eindeutig definierte Code kann nach (1) bis zu 3 Bitfehler korrigieren. Er kann auch durch seine erzeugende Matrix $\boldsymbol{G}$ definiert werden, die von der Paritätsmatrix in ihrer kanonischen Form $\boldsymbol{H} = [\boldsymbol{A}, \boldsymbol{I}_r]$ unmittelbar [3] als $\boldsymbol{G} = [\boldsymbol{I}_k, \boldsymbol{A}^T]$ abgeleitet werden kann. Dabei bedeutet $\boldsymbol{A}^T$ die transponierte Teilmatrix $\boldsymbol{A}$ von $\boldsymbol{H}$ und $\boldsymbol{I}_k$ die Einheitsmatrix vom Grad k. Die Zeilen der Matrix $\boldsymbol{G}$ bilden die Basisvektoren des k-dimensionalen Coderaumes. Ihre linearen Kombinationen über $GF(2)$ ergeben alle Vektoren bzw. Worte des Codes. Für den obigen Golay-Code erhält man demnach die erzeugende Matrix als:

$$\boldsymbol{G} = \left[\begin{array}{cccccccccccc|ccccccccccc} 1&0&0&0&0&0&0&0&0&0&0&0 & 1&1&1&1&1&1&1&1&1&1&1&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0 & 0&0&0&0&1&1&1&1&1&1&1&1 \\ 0&0&1&0&0&0&0&0&0&0&0&0 & 0&1&1&1&0&0&0&1&1&1&1&1 \\ 0&0&0&1&0&0&0&0&0&0&0&0 & 1&0&1&1&0&1&1&0&0&1&1&1 \\ 0&0&0&0&1&0&0&0&0&0&0&0 & 1&1&0&1&1&0&1&0&1&0&1&1 \\ 0&0&0&0&0&1&0&0&0&0&0&0 & 1&1&1&0&1&1&0&1&0&0&1&1 \\ 0&0&0&0&0&0&1&0&0&0&0&0 & 0&0&1&1&1&1&0&0&1&0&1&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0 & 0&1&0&1&0&1&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0 & 0&1&1&0&1&0&1&0&0&1&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&0 & 1&0&0&1&1&0&0&1&0&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&0 & 1&0&1&0&0&0&1&1&1&0&1&1 \\ \hline 0&0&0&0&0&0&0&0&0&0&0&1 & 1&1&0&0&0&1&0&0&1&1&1&1 \end{array}\right] \quad (4)$$

Golay hat auch u.a. die Vermutung geäussert, dass es möglicherweise ausser den früher erwähnten dichtgepackten Codes und dem Code (23, 12, 7) keine perfekten binären Codes mehr geben kann [6]. Die Richtigkeit dieser Vermutung ist aber erst 1973 von *Tietäväinen* bewiesen worden [3]. Der Golay-Code (23, 12, 7) kann also in dieser Hinsicht als einzigartig angesehen werden. Er ist nicht nur theoretisch interessant, sondern auch zur praktischen Anwendung sehr gut geeignet und wird als solcher mit Vorteil verwendet. Es soll daher im folgenden auf einige wichtige, meistens aber nur flüchtig berührte Eigenschaften dieses Codes näher eingegangen werden.

3. Der zyklische Golay-Code

Für das Wertetripel (23, 12, 7) gibt es auch andere Codes, die dem von Golay mit (3) definierten *äquivalent* sind, und zwar in dem Sinne, dass sie in bezug auf Gewichtsverteilung der Codeworte und Fehlerwahrscheinlichkeit gleichwertig sind, sonst aber noch weitere nützliche Eigenschaften besitzen können. Der Begriff Golay-Code kann also als eine Klasse von äquivalenten dichtgepackten Codes aufgefasst werden.

[1]) Marcel J. E. Golay, geb. 1902 in Neuchâtel.

Unter den linearen Codes kommt den *zyklischen* Codes eine besondere Bedeutung zu. Eine zyklische Permutation der Elemente des Codewortes ergibt in diesem Fall wieder ein Codewort. Zur Codierung und Decodierung werden hier nur Schieberegister und verhältnismässig einfache logische Folgeschaltungen benötigt.

Fasst man die Codeworte der Länge n als Polynome vom Grade $\leq n - 1$ auf, deren Koeffizienten aus dem Galois-Körper $GF(2)$ den Codewortelementen

$$< c_1, c_2, ..., c_n > : = c_1 x^{n-1} + c_2 x^{n-2} + ... + c_{n-1} x + c_n$$

entsprechen, so kann der zyklische Golay-Code folgendermassen definiert werden: *der äquivalente zyklische Golay-Code (23, 12, 7) ist ein Hauptideal im Polynomrestklassenring modulo $x^n + 1$ über $GF(2)$ mit $n = 23$, erzeugt durch ein Polynom $g(x)$ vom Grade $r = 11$.* Alle Codeworte, als Elemente des obigen Ideals, müssen dieses Polynom als Faktor enthalten. Es muss auch ein Teiler von $(x^{23} + 1)$ sein, denn aus $x^{23} + 1 = g(x)\, h(x) + r(x)$ folgt $g(x)\, h(x) = r(x) \bmod (x^{23} + 1)$ und, da $r(x)$ von kleinerem Grade als $g(x)$ ist, muss $r(x) = 0$ sein. Die folgende Zerlegung über GF(2) [3]:

$$x^{23} + 1 = (x + 1)(x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1)(x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1)$$

liefert zwei Polynome 11. Grades, die äquivalente zyklische Golay-Codes erzeugen. Diese Polynome sind unzerlegbar (irreduzibel) über GF(2) (siehe z.B. Anhang C in [2]) und zueinander reziprok. Ein zu $g(x)$ reziprokes Polynom, definiert als $x^{11}\, g(x^{-1})$, hat die gleichen Koeffizienten, aber in umgekehrter Reihenfolge. Im vorliegenden Fall sind die Koeffizienten beider Polynome:
$< 101011100011 >$ und $< 110001110101 >$.

Die Multiplikation $\bmod (x^{23} + 1)$ eines Codewortpolynoms

$$c(x) = c_1 x^{22} + c_2 x^{21} + ... + c_{22} x + 1$$

mit x ergibt, da $x^{23} = 1 \bmod (x^{23} + 1)$ ist,

$$c_1 x^{23} + c_2 x^{22} + ... + c_{22} x^2 + c_{23} x = c_2 x^{22} + c_3 x^{21} + ... + c_{23} x + c_1,$$

wieder ein Codewort, mit der zyklischen Permutation der Koeffizienten:

$$\begin{pmatrix} 1, 2, ..., 22, 23 \\ 2, 3, ..., 23, 1 \end{pmatrix}.$$

Durch wiederholte Multiplikation mit x kann man aus dem Polynom $g(x)$ k linear unabhängige Codeworte bzw. -vektoren erhalten, die den k-dimensionalen Code-Unterraum aufspannen, mithin die Zeilen der erzeugenden Matrix $\boldsymbol{G}$ bilden können. Somit erhält man vom ersten der oben angegebenen Polynome $g(x) = x^{11} + x^9 + x^7 + x^6 + x^5 + x + 1$ die erzeugende Matrix des Codes:

$$\boldsymbol{G} = \left[\begin{array}{cccccccccccccccccccccccc} 1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0&0 \\ 0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0&0 \\ 0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0&0 \\ 0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0&0 \\ 0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0&0 \\ 0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0&0 \\ 0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0&0 \\ 0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0&0 \\ 0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0&0 \\ 0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0&0 \\ 0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1 \end{array}\right]$$

Mit linearen Kombinationen der Zeilen kann diese Matrix in die kanonische Form $\boldsymbol{G} = [\boldsymbol{I}_{12}, \boldsymbol{A}]$ übergeführt werden:

$$\boldsymbol{G} = \left[\begin{array}{cccccccccccc|cccccccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1 \\ 0&1&0&0&0&0&0&0&0&0&0&0&1&1&1&1&1&0&0&1&0&0&1 \\ 0&0&1&0&0&0&0&0&0&0&0&0&1&1&0&1&0&0&1&0&1&0&1 \\ 0&0&0&1&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&1 \\ 0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&1&1&0&1&1&0&0 \\ 0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&1&1&0&1&1&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&0&1&1&0&0&1&1&0&1&1 \\ 0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&0&1&1&1&1&0&0 \\ 0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&0&1&1&1&1&0 \\ 0&0&0&0&0&0&0&0&0&1&0&0&0&0&1&0&1&1&0&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1&0 \\ 0&0&0&0&0&0&0&0&0&0&0&1&0&1&0&1&1&1&0&0&0&1&1 \end{array}\right]$$

Daraus folgt die Paritätsmatrix

$$\boldsymbol{H} = \left[\begin{array}{cccccccccccc|cccccccccccc} 1&1&1&1&1&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0 \\ 0&1&1&1&1&1&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0 \\ 1&1&0&0&0&1&1&1&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0 \\ 0&1&1&0&0&0&1&1&1&0&1&1&0&0&0&1&0&0&0&0&0&0&0 \\ 1&1&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0 \\ 1&0&0&1&1&1&0&1&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0 \\ 1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0 \\ 0&1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0 \\ 0&0&1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0 \\ 0&0&0&1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0 \\ 1&1&1&1&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1 \end{array}\right] \tag{5}$$

Das andere Polynom $g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1$ führt zu einem äquivalenten (aber nicht identischen) Code mit der erzeugenden Matrix

$$\boldsymbol{G} = \left[\begin{array}{cccccccccccc|cccccccccccc} 1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0 \\ 0&1&0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1 \\ 0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&0&0 \\ 0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1&0 \\ 0&0&0&0&1&0&0&0&0&0&0&0&0&0&1&1&1&1&0&1&1&0&1 \\ 0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1&0&0 \\ 0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1&0 \\ 0&0&0&0&0&0&0&1&0&0&0&0&0&0&1&1&0&1&1&0&0&1&1 \\ 0&0&0&0&0&0&0&0&1&0&0&0&1&1&0&1&1&1&0&0&0&1&1 \\ 0&0&0&0&0&0&0&0&0&1&0&0&1&0&1&0&1&0&0&1&0&1&1 \\ 0&0&0&0&0&0&0&0&0&0&1&0&1&0&0&1&0&0&1&1&1&1&1 \\ 0&0&0&0&0&0&0&0&0&0&0&1&1&0&0&0&1&1&1&0&1&0&1 \end{array}\right]$$

Tabelle I

Gewicht	Anzahl der Worte
$i-3$	$\binom{i}{3}\binom{23-i}{0}$
$i-2$	$\binom{i}{2}\binom{23-i}{0}$
$i-1$	$\binom{i}{1}\binom{23-i}{0}+\binom{i}{2}\binom{23-i}{1}$
i	$\binom{i}{0}\binom{23-i}{0}+\binom{i}{1}\binom{23-i}{1}$
$i+1$	$\binom{i}{0}\binom{23-i}{1}+\binom{i}{1}\binom{23-i}{2}$
$i+2$	$\binom{i}{0}\binom{23-i}{2}$
$i+3$	$\binom{i}{0}\binom{23-i}{3}$

4. Gewichtsverteilung und Codeerweiterung

Zur Berechnung gewisser mit dem Code zusammenhängender Wahrscheinlichkeiten ist die Kenntnis der Gewichtsverteilung notwendig. Das Gewicht w eines Codewortes ist gleich der Anzahl von Stellen, die nicht gleich null sind. Die Gewichtsverteilung ist eine auf der Menge der Gewichte $\{w\}$ definierte Funktion $A(w)$, deren Werte der Anzahl der Codeworte vom Gewicht w gleich sind. Sie stellt auch die Verteilung der Hammingschen Distanz der Codeworte vom Nullwort dar.

Um diese Verteilung für den Golay-Code zu bestimmen, beachte man, dass je nachdem, ob die Bitfehler auf Nullen oder Einsen im Codewort entfallen, jede n-dimensionale Kugel um ein Codewort vom Gewicht i in die Gewichtsklassen von Tabelle I zerlegt werden kann. Da der betrachtete Code dichtgepackt ist, müssen alle Beiträge der Kugeln um die Codeworte vom Gewicht $(j-3), \ldots, (j+3)$ zur Gewichtsklasse j aller möglichen Worte der Länge $n = 23$ deren Anzahl $\binom{23}{j}$ ergeben, so dass

$$A(j-3)\binom{26-j}{3} + A(j-2)\binom{25-j}{2} + A(j-1)\left[24-j+(j-1)\binom{24-j}{2}\right] +$$
$$+ A(j)\left[1+j(23-j)\right] + A(j+1)\left[j+1+\binom{j+1}{2}(22-j)\right] + A(j+2)\binom{j+2}{2} + A(j+3)\binom{j+3}{3} = \binom{23}{j}.$$

Mit der Substitution $j = w - 3$ folgt daraus die Rekursionsbeziehung

$$A(w)\binom{w}{3} + A(w-1)\binom{w-1}{2} + A(w-2)\left[w-2+\binom{w-2}{2}(25-w)\right] + A(w-3)\left[1+(w-3)(26-w)\right] +$$
$$+ A(w-4)\left[27-w+(w-4)\binom{27-w}{2}\right] + A(w-5)\binom{28-w}{2} + A(w-6)\binom{29-w}{3} = \binom{23}{w-3}. \tag{6}$$

Wie schon erwähnt, müssen alle Codewortpolynome eines zyklischen Codes, im besonderen also auch die Zeilen der erzeugenden Matrix $\boldsymbol{G}$, das Polynom $g(x)$ als gemeinsamen Teiler enthalten. Wenn man nun z. B. die zwei letzten Zeilen der Matrix (4) ins Auge fasst, so kann man sich leicht überzeugen (z. B. mit Hilfe des euklidschen Algorithmus), dass diese teilerfremd sind. Folglich ist der von *Golay* in [4] angegebene perfekte Code *nicht zyklisch*. Die beiden äquivalenten Codes hingegen, mit gleichen Parametern $(n, k, d) = (23, 12, 7)$, die die Bedingung (2) erfüllen, sind zugleich dichtgepackt und zyklisch.

Mit $A(0) = 1$, $A(1) = \ldots = A(6) = 0$ erhält man aus (6) nacheinander die weiteren Werte: $A(7) = 253$, $A(8) = 506$, $A(9) = A(10) = 0$, $A(11) = 1288$.

Weitere Berechnungen erübrigen sich, weil in einem Gruppencode jedem Codewort mit dem Gewicht w ein Codewort mit dem komplementären Gewicht $n - w$, das durch die Addition des Einswortes zum ersteren entsteht, umkehrbar eindeutig zugeordnet werden kann. Es gilt also $A(w) = A(n - w)$, so dass $A(12) = A(11)$, $A(13) = A(10)$ usw.

Der Golay-Code (23, 12, 7) kann durch Hinzunahme einer zusätzlichen, über das ganze Codewort erstreckten Paritäts-

stelle zu einem Code (24, 12, 8) erweitert werden. Bei gleichbleibender Anzahl der k Informationsstellen wird somit die Länge der Codeworte und das Gewicht aller Codeworte mit ungeradzahligem Gewicht, mithin auch die minimale Distanz d, um 1 erhöht, was allerdings die Anzahl der korrigierbaren Fehler nicht vergrössert.

Es ist leicht einzusehen, dass dadurch die Paritätsmatrix des ursprünglichen Codes um eine Zeile und eine Spalte erweitert wird. So erhält man z. B. aus der Matrix (5) des zyklischen Golay-Codes (23, 12, 7) die folgende Paritätsmatrix des erweiterten Golay-Codes (24, 12, 8):

$$H' = \left[\begin{array}{cccccccccccc|cccccccccccc|c}
1&1&1&1&1&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&1&1&1&1&1&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&0\\
1&1&0&0&0&1&1&1&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&1&1&0&0&0&1&1&1&0&1&1&0&0&0&1&0&0&0&0&0&0&0&0&0\\
1&1&0&0&1&0&0&0&1&1&1&1&0&0&0&0&1&0&0&0&0&0&0&0&0\\
1&0&0&1&1&1&0&1&0&1&0&1&0&0&0&0&0&1&0&0&0&0&0&0&0\\
1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&0\\
0&1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0\\
0&0&1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&1&0&1&1&0&1&1&1&1&0&0&0&0&0&0&0&0&0&1&0&0&0\\
1&1&1&1&0&0&1&0&0&1&0&1&0&0&0&0&0&0&0&0&0&0&1&0&0\\
\hline
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1
\end{array}\right]$$

Ein solcher Code ist offenbar nicht mehr dichtgepackt (und auch nicht mehr zyklisch), hat aber andere interessante Eigenschaften (z. B. Zusammenhänge mit anderen Codearten, nützliche Automorphismen u. a.), auf die hier allerdings nicht näher eingegangen werden kann. Es sei in diesem Zusammenhang nur auf [3] verwiesen, wo besonders der erweiterte Golay-Code ausführlich behandelt wird.

Die Gewichtsverteilung des erweiterten Golay-Codes kann von derjenigen des perfekten Golay-Codes einfach abgeleitet werden, indem alle Werte $A(w)$ für ungerades w zu den Werten $A(w+1)$ hinzuaddiert und $A(w) = 0$ gesetzt werden. Somit können die Gewichtsverteilungen für den dichtgepackten und den erweiterten Golay-Code in Tabelle II zusammengestellt werden.

5. Empfangswahrscheinlichkeit

Die Wahrscheinlichkeit, dass ein *gesendetes* Codewort richtig empfangen wird, ist gleich derjenigen, dass nicht mehr als 3 Bitfehler im Codewort auftreten. Unter der Voraussetzung der stochastischen Unabhängigkeit der Bitfehler innerhalb eines Codewortes und dass die Bitfehlerrate p als Wahrscheinlichkeit eines Fehlers an einer beliebigen Stelle des Codewortes angenommen werden kann, ergibt sich für den Golay-Code mit $q = 1 - p$

$$P_1 = \sum_{i=0}^{3} \binom{n}{i} p^i q^{n-i}. \qquad (7)$$

Dabei ist für den perfekten Golay-Code $n = 23$ und für den erweiterten $n = 24$ zu setzen.

Das Ereignis, dass ein *nicht* gesendetes Codewort trotzdem, infolge von Bitfehlern, unerwünschterweise empfangen wird, bedeutet z. B. in beweglichen Fernmeldesystemen einen störenden falschen Anruf des betroffenen Teilnehmers. Zur Ermittlung der Wahrscheinlichkeit P_2 eines solchen Ereignisses muss die Distanzverteilung der Codeworte berücksichtigt werden.

Aus der Definition der Hammingschen Distanz $h(c, c_0)$ und des Gewichtes $w(c)$ der Codeworte eines binären Gruppencodes über $GF(2)$ folgt, dass $h(c, c_0) = w(c + c_0)$.

Es ist leicht einzusehen, dass die Abbildung $f\colon c \to c + c_0$ eine Bijektion von $C = \{c\}$ auf sich ist. Die Anzahl der Codeworte mit der Distanz h von c_0 ist mithin der Anzahl der Codeworte vom Gewicht w gleich. Die Distanzverteilung ist folglich gegenüber f invariant und für jedes Codewort c_0 mit der Gewichtsverteilung $A(w)$ identisch. Im besonderen ist auch die minimale Distanz d gleich dem minimalen Gewicht.

Die gesuchte Wahrscheinlichkeit P_2 ist gleich der Wahrscheinlichkeit, dass ein Codewort c_0 empfangen wird, unter der Bedingung, dass ein Codewort mit der Distanz $i \neq 0$ gesendet wurde, erstreckt auf alle möglichen Werte $i = d, \ldots, n$, was offenbar exklusiven Ereignissen entspricht. Es ist also

$$P_2 = \sum_{i=d}^{n} Pr\{c_0 \mid i\}\, Pr\{i\}$$

Infolge der Bitfehler kann die Distanz des gesendeten Codewortes geändert, im besonderen auch vermindert werden. Wenn sie dadurch bis auf höchstens 3 herabgesetzt wird, so wird das empfangene Wort als das Codewort c_0 identifiziert, da der Golay-Code bis zu 3 Bitfehler zu korrigieren vermag. Dies kann folgendermassen erfolgen:

1. Es können in einem mit der Distanz i gesendeten Codewort genau i Bitfehler auftreten, die diese Distanz auf 0 herabsetzen, mit der Wahrscheinlichkeit

$$p^i q^{n-i}$$

2. Die Anzahl der Bitfehler innerhalb der obigen i Stellen kann $i - j$ betragen, mit $j \leq 3$, mit der Wahrscheinlichkeit

$$\binom{i}{i-j} p^{i-j} q^{n-(i-j)}$$

3. Die Anzahl der Bitfehler umfasst die obigen i Stellen und beträgt $i + j$ mit $j \leq 3$, mit der Wahrscheinlichkeit

$$\binom{n-i}{j} p^{(i+j)} q^{n-(i+j)}$$

Diese Fälle schliessen einander aus, so dass die bedingte Wahrscheinlichkeit

$$Pr\{c_0 \mid i\} = p^i q^{n-i} + \sum_{j=1}^{3} \binom{i}{j} p^{i-j} q^{n-(i-j)} + \sum_{j=1}^{3} \binom{n-j}{j} p^{i+j} q^{n-(i+j)}$$

ist.

Tabelle II

Gewicht w	Anzahl der Codeworte $A(w)$ im Golay-Code: (23, 12, 7)	(24, 12, 8)
0	1	1
1, ..., 6	0	0
7	253	0
8	506	759
9, 10	0	0
11	1288	0
12	1288	2576
13, 14	0	0
15	506	0
16	253	759
17, ..., 22	0	0
23	1	0
24	0	1
insgesamt	4096	4096

Die Wahrscheinlichkeit dafür, dass ein Codewort mit der Distanz i (einschliesslich des Nullwortes) gesendet wird, beträgt

$$Pr\{i\} = \frac{A(i)}{2^{12}}$$

Somit ergibt sich für die Wahrscheinlichkeit des falschen Anrufes im Golay-Code der Ausdruck

$$P_2 = 2^{-12} \sum_{i=d}^{n} A(i)\, p^i\, q^{n-i} \left[1 + \sum_{j=1}^{3} \binom{i}{j} \left(\frac{q}{p}\right)^j + \sum_{j=1}^{3} \binom{n-i}{j} \left(\frac{p}{q}\right)^j\right] \quad (8)$$

Für den dichtgepackten Code ist in diesem Ausdruck $n = 23$ und für den erweiterten $n = 24$ einzusetzen. Die Werte der Koeffizienten $A(i)$ sind dabei der Tabelle II für $A(w)$ mit $i = w$ zu entnehmen.

Beide Formeln (7) und (8) ergeben für den perfekten Golay-Code grössere Werte als für den erweiterten. Allerdings ist die Differenz im Fall der Formel (7) unerheblich, so dass beide Codes in bezug auf Decodierung als fast gleichwertig gelten können. Für den Ausdruck (8) hingegen ist die Differenz beträchtlich grösser. Der erweiterte Golay-Code ist also bezüglich der Wahrscheinlichkeit unerwünschter Anrufe günstiger.

Literatur

[1] *H. Ohnsorge:* Die Anwendung von Galoiskörpern in der Codierungstheorie, Bull. SEV, 64(1973)8, pp. 493...499.

[2] *W. W. Peterson* and *E. J. Weldon:* Error-correcting codes, Second edition. Cambridge Massachusetts/London, MIT Press, 1978.

[3] *F. J. Mac Williams* and *N. J. A. Sloane:* The theory of error-correcting codes, Amsterdam/New York/Oxford, North-Holland Publishing Co., 1978.

[4] *M. J. E. Golay:* Notes on digital coding, Proc. IRE, 37(1949)6, p. 657.

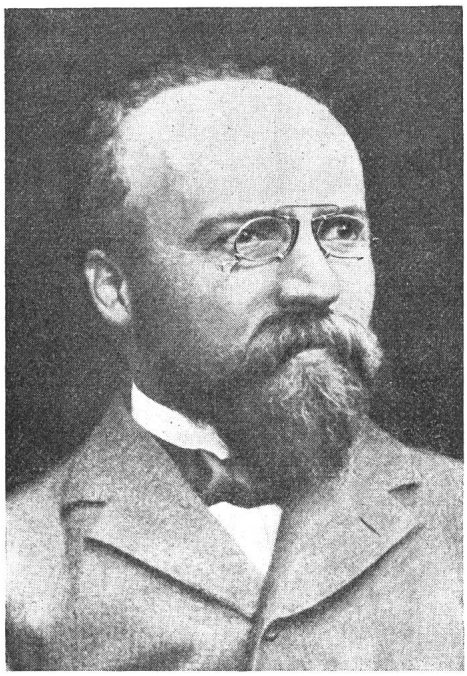
[5] *M. J. E. Golay:* Notes on the penny-weighing problem, lossless symbol coding with nonprimes, etc. IRE Transactions on Information Theory 4(1958)3, p. 103...109.

[6] *M. J. E. Golay:* Binary codes. IRE Transactions on Information Theory 1(1954)4, p. 23...28.

Adresse des Autors

Joseph Fabijanski, dipl. Ing., Rebenstrasse 74, 8041 Zürich.

Carl Emil Krarup 1872–1909



Königliche Bibliothek Kopenhagen

Als sich Ende des 19. Jahrhunderts die Telefonnetze auf immer grössere Gebiete ausdehnten, machte sich die zu grosse Dämpfung der Leitungen in zunehmendem Mass unangenehm bemerkbar. Heaviside hatte dieses Problem vorausgesehen und verschiedene Wege zur Erhöhung der Selbstinduktion und damit Verkleinerung der Dämpfung vorgeschlagen. Das Krarupkabel stellt eine solche Lösung dar.

Carl Emil Krarup, Sohn eines Textilkaufmannes, wurde am 12. Oktober 1872 in Kopenhagen geboren. Mit 24 Jahren schloss er sein Studium als Bauingenieur ab und arbeitete 2 Jahre lang beim Kopenhagener Amt für Strassen und Kanalisation. Darauf trat er als technischer Ingenieur-Aspirant zum staatlichen Telegrafenwesen über, machte 1901 Studien am Physikalischen Institut in Würzburg, worauf er am 1. Dezember 1902 zum Telegrafeningenieur ernannt wurde.

Zu jener Zeit schrieb die Universität Kopenhagen eine Preisaufgabe aus über die Selbstinduktion elektrischer Leitungen. Krarup beteiligte sich am Wettbewerb, wurde ausgezeichnet und kam dadurch ins Gespräch mit Professor Pedersen von der Universität. Dieser war überzeugt, dass Krarup mit seinem Vorschlag auf dem rechten Weg sei, und förderte ihn. Schon im Spätherbst 1902 fabrizierte die Firma Felten und Guillaume nach Krarups Angaben ein erstes, 4 km langes Kabel, das durch den Oeresund verlegt wurde. Beim Krarupkabel sind die feinen Kupferleiter mit etwa 0,2 bis 0,3 mm dickem Eisendraht oder 0,15 mm dickem, etwa 3 mm breitem Eisenband umwickelt, was eine beträchtliche Reduktion der Dämpfung bewirkt. Ein Jahr später folgte ein 20 km langes Seekabel zwischen Dänemark und Deutschland (Fehmarn-Belt). Von da an fanden Krarupkabel für Telefon- und später auch für Telegrafenleitungen regelmässig Verwendung.

1906 rückte Krarup zum Leiter der technischen Abteilung der Telegrafendirektion auf. Er war bei radiotelegrafischen Versuchen auf den Lofoten (Norwegen) beteiligt, wirkte als Berater der Telegrafenverwaltungen von Island, der Färöer-Inseln sowie in Baku. Er war Mitglied der Meterkommission und spielte auch im IEC eine Rolle. Mitten aus einer rastlosen Tätigkeit wurde er am 30. Dezember 1909 in Kopenhagen nach kurzer Krankheit durch den Tod abberufen. Über sein Privatleben ist ausser seiner Heirat am 23. August 1904 nur wenig bekannt. Er soll sehr beliebt gewesen sein.

Die Krarupkabel wurden weiter entwickelt und fanden bis etwa 1935 breite Anwendung. Die gleichmässige Verteilung der Selbstinduktion über die ganze Kabellänge, der gleichbleibende Kabeldurchmesser und die leichte Reparaturmöglichkeit galten lange als Vorteil gegenüber der fast gleichzeitig erfundenen und dem gleichen Zweck dienenden Pupin-Spule. Diese, etwa ab 1920 gebaut, hat später das teurere, etwas schwerere und dickere Krarupkabel verdrängt.

H. Wüger