Codierung und Decodierung zyklischer Quantencodes

Markus Grassl und Thomas Beth

Institut für Algorithmen und Kognitive Systeme (IAKS)
Universität Karlsruhe
Am Fasanengarten 5
76 128 Karlsruhe
Telefon: 0721/608-42 05
e–mail: EISS_Office@ira.uka.de

Wir betrachten innerhalb der fehlerkorrigierenden Quantencodes die Teilklasse der zyklischen Quantencodes insbesondere unter dem Gesichtspunkt der Codierung und Decodierung. Die zyklische Struktur der Codes ermöglicht effiziente Algorithmen zur Codierung und Decodierung. Dabei können Ansätze aus der „klassischen“ Schaltungstechnik (z. B. rückgekoppelte lineare Schieberegister) übernommen werden.

1. Einleitung

Vor etwa drei Jahren wurde erstmals gezeigt, daß mit Hilfe von *Quantenrechnern* Probleme in polynomialer Zeit gelöst werden können, für die alle bisher bekannten klassischen Algorithmen einen exponentiellen Aufwand besitzen (z. B. das Faktorisieren großer Zahlen, cf. [Sho94]). Die Suche eines Elementes in einer unstrukturierten Menge mit N Elementen kann auf einem Quantenrechner in $O(\sqrt{N})$ erfolgen, wohingegen der Aufwand auf einem klassischen Rechner linear ist (cf. [Gro97]).

Eines der größten Hindernisse auf dem Weg zur Realisierung von Rechnern, welche auf den Prinzipien der Quantenmechanik basieren, schien jedoch die Tatsache zu sein, daß schon kleinste äußere Einflüsse, wie die Interaktion mit einzelnen Photonen, katastrophale Fehler in einem Quantensystem bewirken können. Ansätze aus der klassischen Codierungstheorie sind nicht direkt übertragbar; denn dort ist ein wesentliches Prinzip, die Information auf mehrere Kopien zu verteilen, um Fehler entdecken und korrigieren zu können. Allgemeine Quantenzustände können aber nicht kopiert werden, das verbietet das sogenannte *no–cloning*–Theorem [WoZu82].

Vor knapp zwei Jahren wurde der erste fehlerkorrigierende Code für Quantensysteme vorgestellt und damit gezeigt, daß auch Quantenzustände gegen Fehler geschützt werden können [Sho95]. Mittlerweile hat sich eine Theorie der Codes für Quantensysteme entwickelt [KnLa97]. Allerdings sind noch sehr wenige Algorithmen für die Durchführung der eigentlichen Fehlerkorrektur bekannt.

In unserem Beitrag betrachten wir daher, nach einer kurzen Einführung in die Begriffe des *Quantum Computing*, die Teilklasse der zyklischen Quantencodes unter dem Gesichtspunkt der Codierung und Decodierung. Es zeigt sich, daß die aus der zyklischen Struktur der Codes resultierenden algebraischen Eigenschaften effiziente Algorithmen zur Codierung und Decodierung ermöglichen.

2. Einige Grundlagen

Zunächst soll knapp auf die wichtigsten Begriffe und Notationen aus dem Bereich des *Quantum Computing* eingegangen werden (siehe hierzu auch die Beiträge [KBG98, Wer98] in diesem Tagungsband).

2.1 Quantenregister

In Analogie zum klassischen Bit, das die Werte 0 und 1 annehmen kann, wird ein Quantenbit (*Qubit*) modelliert als eine komplexe Linearkombination der normierten, orthogonalen Basisvektoren $|0\rangle$ und $|1\rangle$:

$$|q\rangle = \alpha\,|0\rangle + \beta\,|1\rangle \qquad \text{mit } \alpha, \beta \in \mathbb{C},\ |\alpha|^2 + |\beta|^2 = 1.$$

Die Normierungsbedingung leitet sich ab aus der Tatsache, daß bei einer Messung des Qubits die Werte 0 und 1 jeweils mit einer Wahrscheinlichkeit von $|\alpha|^2$ bzw. $|\beta|^2$ gemessen werden.

Ein System mit N Qubits, das einem klassischen Register der Länge N entspricht, wird modelliert als das Tensorprodukt der zweidimensionalen Vektorräume der einzelnen Qubits, d. h. als ein 2^N–dimensionaler komplexer Vektorraum mit Basisvektoren

$$|b_1\rangle \otimes \ldots \otimes |b_N\rangle =: |b_1 \ldots b_N\rangle = |\boldsymbol{b}\rangle \qquad \text{mit } b_i \in \{0, 1\}.$$

2.2 Quantengatter

Die Operationen auf Quantenzuständen werden beschrieben durch unitäre Matrizen. Somit bleibt die Normierung erhalten. In Analogie zur digitalen Schaltungstechnik wird beispielsweise das NOT–Gatter, das die Zustände $|0\rangle$ und $|1\rangle$ vertauscht, beschrieben durch

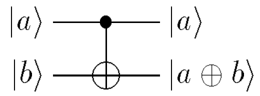
$$NOT := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Außer dieser „klassischen“ Operation sind auf Qubits beliebige unitäre Operationen zulässig, z. B.

$$H := \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \qquad \text{und} \qquad \theta := \frac{1}{2} \begin{pmatrix} i-1 & i-1 \\ i+1 & -(i+1) \end{pmatrix}.$$

Neben diesen Ein–Qubit–Operationen spielt das sogenannte *controlled not* ($CNOT$) eine wichtige Rolle. Es entspricht einem Gatter mit zwei Eingängen. Ein Eingang wird übernommen, der andere Ausgang ist die XOR–Verknüpfung der Eingänge. Das $CNOT$–Gatter ist gegeben durch:

$$CNOT := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$



Rechts ist die Notation des $CNOT$–Gatters als Quantenschaltkreis angegeben. Jede der Leitungen entspricht einem Qubit. Der Punkt deutet an, daß die Operation auf der unteren Leitung nur dann ausgeführt wird, wenn die obere Leitung 1 ist, d. h., auf $|b\rangle$ wird genau dann eine NOT–Operation ausgeführt, wenn sich $|a\rangle$ im Zustand $|1\rangle$ befindet. (Mehr zum Thema Quantengatter und Quantenschaltkreise findet sich beispielsweise in [BBC95].)

2.3 Fehlermodell

Durch Wechselwirkung mit der Umgebung (z. B. Absorption/Emission von Photonen) kann der Zustand in einem Quantensystem gestört werden. Ähnlich wie in der klassischen Codierungstheorie wird auch hier davon ausgegangen, daß Fehler auf einzelne Stellen (Qubits) beschränkt sind. Der Fehler auf diesen Stellen kann durch eine lineare Operation, die nicht notwendigerweise unitär sein muß, modelliert werden. Dabei genügt es, sogenannte Bitfehler und Phasenfehler (sowie deren Kombination) korrigieren zu können (cf. [KnLa97]). Ein Bitfehler entspricht der klassischen Invertierung eines Bits. Beim Phasenfehler, der keine klassische Entsprechung findet, wird der Koeffizient des Zustands $|1\rangle$ negiert. Insgesamt können diese elementaren Fehleroperatoren modelliert werden durch die Identität sowie die Pauli–Matrizen

$$\sigma_x := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad \sigma_y := \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \quad \text{und} \quad \sigma_z := \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad (\text{mit } i^2 = -1).$$

Dabei entspricht σ_x dem Bitfehler und σ_z dem Phasenfehler. Ein Fehler auf einem Quantenregister der Länge N ist dann ein Tensorprodukt dieser Matrizen.

3. Quantencodes und Binärcodes

Die Grundidee der fehlerkorrigierenden Quantencodes besteht darin, die Information so in einem 2^k–dimensionalen Unterraum („Coderaum“) eines 2^N–dimensionalen Raumes zu speichern, daß eine bestimmte Anzahl von Fehlern entdeckt und korrigiert werden kann (siehe Bild 1). Es gilt

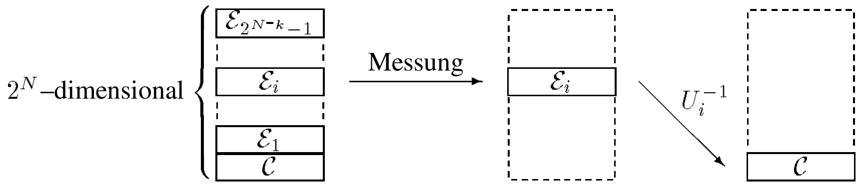


Bild 1: Der gesamte 2^N–dimensionale Raum wird in den 2^k–dimensionalen Coderaum $\mathcal{C}$ sowie verschiedene Fehlerräume $\mathcal{E}_i = U_i\mathcal{C}$ unterteilt. Durch unvollständige Messung wird eine Projektion auf einen dieser Räume durchgeführt. Anschließend findet eine Rücktransformation auf den Coderaum statt.

nun, den Coderaum geeignet zu wählen. Zunächst wird eine Konstruktion für Quantencodes angegeben, die auf linearen Binärcodes basiert (cf. [Ste96]).

Satz 3.1 *Seien $C_1 = [N, k_1, d_1]$ und $C_2 = [N, k_2, d_2]$ lineare Binärcodes derselben Länge mit $C_2^\perp \le C_1$. Ferner sei $\mathcal{W} = \{\boldsymbol{w}_1, \ldots, \boldsymbol{w}_K\}$ ein Repräsentantensystem für $C_1/C_2^\perp$.*

Dann ist durch die $K = 2^{k_1-(N-k_2)}$ orthogonalen Zustände

$$|\underline{\boldsymbol{i}}\rangle = \frac{1}{\sqrt{|C_2^\perp|}} \sum_{\boldsymbol{c}\in C_2^\perp} |\boldsymbol{c} + \boldsymbol{w}_i\rangle \tag{1}$$

ein Quantencode der Länge N und Dimension K gegeben. Dieser Code kann $(d_1-1)/2$ Bitfehler und $(d_2-1)/2$ Phasenfehler korrigieren.

Korollar 3.2 *Ist C ein schwach selbstdualer Binärcode, d. h. $C \le C^\perp$, so kann aus ihm nach Satz3.1 mit $C_1 = C_2 = C^\perp$ ein Quantencode konstruiert werden.*

Die Grundidee dieser Konstruktion ist, daß die Hadamardtransformation H sowohl Bit– und Phasenfehler als auch Code und Dualcode vertauscht. Somit können zunächst die Bitfehler mit Hilfe eines Decodieralgorithmus für den Code C_1 und nach einer Hadamardtransformation die ursprünglichen Phasenfehler als Bitfehler bzgl. des Codes C_2 korrigiert werden. In [BeGr96] wurde gezeigt, daß die Menge $\mathcal{W}$ allgemeiner gewählt werden kann. Die Decodierung der Phasenfehler muß dann etwas modifiziert werden, basiert aber weiterhin auf der Dualität zwischen Bitfehlern und Phasenfehlern.

Zyklische Quantencodes können ausgehend von geeignet gewählten zyklischen Binärcodes konstruiert werden, da sich die Eigenschaft der Invarianz unter zyklischer Verschiebung direkt von Binärcodes auf Quantencodes überträgt.

Satz 3.3 *Seien $g_1(x)$ und $g_2(x)$ Teiler von $x^N - 1$ im Polynomring über $GF(2)$ mit $g_1(x)|g_2(x)$. Dann erfüllen die Codes C_1 mit Generatorpolynom $g_1(x)$ und $C_2^\perp$ mit Generatorpolynom $g_2(x)$ die Bedingungen von Satz 3.1.*

Unter den zyklischen Codes erlauben BCH–Codes eine relativ effiziente Decodierung. Außerdem kann bei der Decodierung auch eventuell vorhandene Information über die Position der Fehler (*erasures*) berücksichtigt werden. Dies überträgt sich direkt auf (binäre) Quanten–BCH–Codes (cf. [GBP97]). Diese $\mathcal{Q}\mathrm{BCH}$–Codes lassen sich über die Nullstellenmengen der zugrundeliegenden binären BCH–Codes charakterisieren.

Satz 3.4 (BCH–Codes für $\mathcal{Q}\mathrm{BCH}$–Codes) *Sei C ein binärer BCH–Code der Länge N. Für die Nullstellenmenge $\mathcal{I}_C$ gelte*

$$\forall i : (i \in \mathcal{I}_C \Longrightarrow (-i \bmod N) \notin \mathcal{I}_C)\,.$$

Dann ist der duale Code $C^\perp$ schwach selbstdual und es kann ein $\mathcal{Q}\mathrm{BCH}$–Code konstruiert werden.

4. Quantencodes und Codes über $GF(4)$

4.1 Konstruktion von Quantencodes aus Codes über $GF(4)$

Die bislang allgemeinste Konstruktion von fehlerkorrigierenden Quantencodes basiert auf additiven Codes über $GF(4)$ (cf. [Got96, CRSS97, BeGr98]). Diese Quantencodes sind charakterisiert durch ihre (punktweise) Stabilisatorgruppe innerhalb der Gruppe, die von Tensorprodukten von Pauli–Matrizen erzeugt wird. Jeder solchen abelschen Stabilisatorgruppe entspricht ein additiv abgeschlossener Code über $GF(4)$. Dabei stehen die Elemente $\{0, 1, \omega, \overline{\omega}\}$ von $GF(4)$ (mit $\overline{\omega} = \omega^2 = \omega + 1$) und die Pauli–Matrizen in der folgenden Beziehung:

$$0 \mathrel{\hat{=}} id, \qquad 1 \mathrel{\hat{=}} \sigma_x, \qquad \omega \mathrel{\hat{=}} \sigma_z, \qquad \overline{\omega} \mathrel{\hat{=}} \sigma_y. \tag{2}$$

Vektoren der Länge N stehen in Korrespondenz zu Tensorprodukten von N Matrizen. Umgekehrt kann auch ausgehend von einem Code über $GF(4)$ eine Gruppe definiert werden. Damit die Gruppe abelsch ist, muß der Code die folgende Bedingung erfüllen:

Satz 4.1 *Es sei C ein additiv abgeschlossener Code der Länge N über $GF(4)$. Ist C selbstorthogonal, d. h. $C \leq \overline{C^\perp}$, wobei $\overline{C^\perp}$ die komponentenweise Konjugation $x \mapsto x^2$ über $GF(4)$ des Dualcodes $C^\perp$ bezeichnet, so ist die zugehörige Gruppe abelsch.*

Die Basiszustände des so konstruierten Quantencodes werden via einer Mittelungsoperation über die Bahnen von geeignet gewählten Startvektoren $|\boldsymbol{b}_i\rangle$ unter der Stabilisatorgruppe $\mathcal{S}$ gewonnen, d. h.

$$|\underline{\boldsymbol{i}}\rangle = \frac{1}{\sqrt{|\mathcal{S}|}} \sum_{g \in \mathcal{S}} g \cdot |\boldsymbol{b}_i\rangle\,. \tag{3}$$

Selbstorthogonale zyklische Codes können wiederum anhand des Generatorpolynoms charakterisiert werden.

Satz 4.2 *Sei $g(x) \cdot h(x) = x^N - 1$ im Polynomring über $GF(4)$ mit $\overline{h(x)}|g(x)$. Dann ist der zyklische Code mit Generatorpolynom $g(x)$ selbstorthogonal und es kann ein zyklischer Quantencode konstruiert werden.*

4.2 Beispiel

Obiges soll anhand des $[[5,1,3]]$–Quanten–Hamming–Codes illustriert werden. Es ist der kürzeste Code, der ein Qubit codieren und einen Fehler korrigieren kann (cf. [LMPZ96]). Die additiven Erzeuger $\boldsymbol{g}_i$ des zugehörigen Codes über $GF(4)$ sowie die korrespondierenden Erzeuger g_i der Stabilisatorgruppe $\mathcal{S}$ sind gegeben durch:

$$\begin{array}{l} \boldsymbol{g}_1 = (1 \quad 0 \quad 1 \quad \overline{\omega} \quad \overline{\omega}) \\ \boldsymbol{g}_2 = (\omega \quad 0 \quad \omega \quad 1 \quad 1) \\ \boldsymbol{g}_3 = (0 \quad 1 \quad \overline{\omega} \quad \overline{\omega} \quad 1) \\ \boldsymbol{g}_4 = (0 \quad \omega \quad 1 \quad 1 \quad \omega) \end{array} \quad \text{und} \quad \begin{array}{l} g_1 = \sigma_x \otimes id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y \\ g_2 = \sigma_z \otimes id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x \\ g_3 = id \otimes \sigma_x \otimes \sigma_y \otimes \sigma_y \otimes \sigma_x \\ g_4 = id \otimes \sigma_z \otimes \sigma_x \otimes \sigma_x \otimes \sigma_z \end{array}$$

Geeignete Startvektoren sind z. B. $|\boldsymbol{b}_0\rangle = |00000\rangle$ und $|\boldsymbol{b}_1\rangle = |00010\rangle$. Ein Teil des Quantenschaltkreis zur Codierung eines Qubits ist in Bild 2 angegeben. (Man beachte, daß die Generatoren g_2 und g_4 jeweils durch zyklische Verschiebung aus den Generatoren g_1 und g_3 hervorgehen, was sich auch im Quantenschaltkreis widerspiegelt.) Dabei wird Formel (3) in der Form

$$|\underline{\boldsymbol{i}}\rangle = \frac{1}{\sqrt{2^4}} \sum_{i_1,i_2,i_3,i_4 \in \{0,1\}} g_1^{i_1} g_2^{i_2} g_3^{i_3} g_4^{i_4} \cdot |\boldsymbol{b}_i\rangle$$

verwendet.

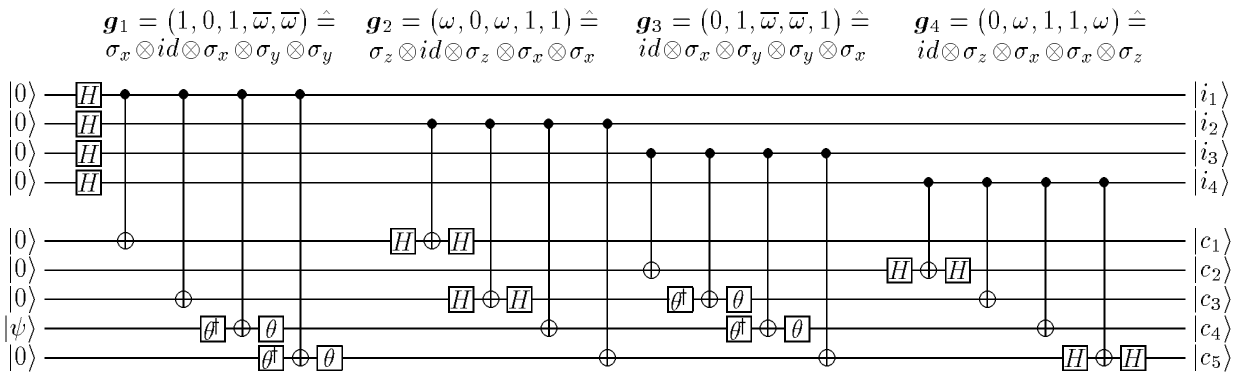


Bild 2: Quantenschaltkreis zur Codierung des Zustands $|\psi\rangle$ unter Verwendung des $[[5,1,3]]$–Quanten–Hamming–Codes. Die Hilfsstellen $|i_1\rangle\,|i_2\rangle\,|i_3\rangle\,|i_4\rangle$ sind noch mit dem codierten Zustand $|c_1\rangle\,|c_2\rangle\,|c_3\rangle\,|c_4\rangle\,|c_5\rangle$ verschränkt. Diese Verschränkung wird durch einen nachfolgenden Schaltkreis aufgehoben.

5. Decodierung zyklischer Quantencodes

5.1 Syndromberechnung

Das Spektrum der Operatoren in der Stabilisatorgruppe $\mathcal{S}$ ist $\{-1,1\}$. Die Zustände des Quantencodes liegen alle im Schnitt der Eigenräume zum Eigenwert 1. Ein erkennbarer Fehler führt nun dazu, daß der gestörte Zustand im Eigenraum zum Eigenwert -1 von mindestens einem der Operatoren liegt. Ein Fehler kann also erkannt werden, indem für jeden der Generatoren der Stabilisatorgruppe festgestellt wird, ob der Zustand im Eigenraum zum Eigenwert $+1$ oder -1 liegt. Dies kann mit Hilfe des in Bild 3 gezeigten Quantenschaltkreises erfolgen. Das Syndrom $\boldsymbol{s} = s_1\, s_2\, s_3\, s_4$

entspricht dabei dem „klassischen“ Syndrom bzgl. der Generatoren $\boldsymbol{g}_i$ des $GF(4)$–Codes. Das Syndrom $\boldsymbol{s}$ ist ein Binärvektor der Länge vier, kann aber auch als Vektor der Länge zwei über $GF(4)$ interpretiert werden, wenn jedes Element von $GF(4)$ als zweistelliger Binärvektor dargestellt wird.

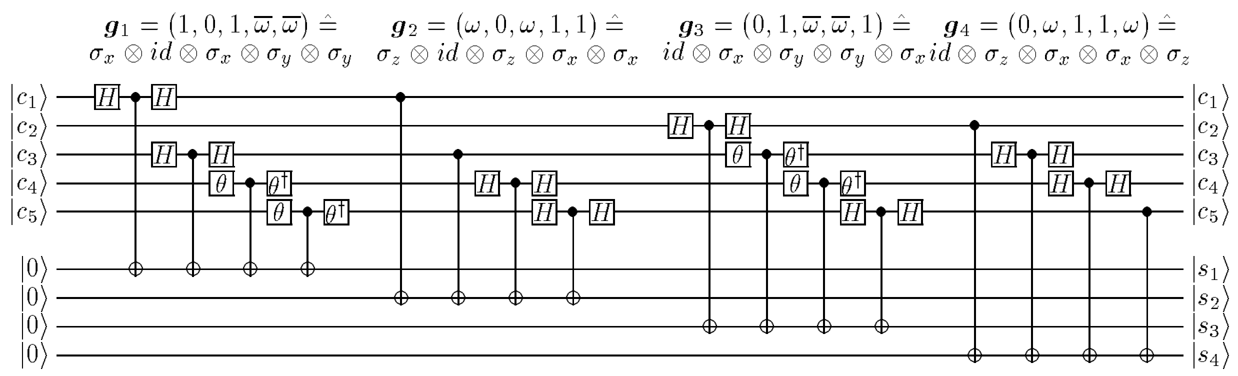


Bild 3: Berechnung des Syndroms mittels einer *non–demolition*–Messung der Generatoren g_i der Stabilisatorgruppe des Codes. Man beachte die Dualität zur Codierungsschaltung in Bild 2.

Nun kann das Syndrom gemessen werden, wodurch entsprechend Bild 1 eine Projektion auf einen der Fehlerräume stattfindet. Nachdem (klassisch) der zugehörige Fehlervektor über $GF(4)$ bestimmt wurde, kann der Fehler durch Anwendung der entsprechenden Operation (vgl. (2)) korrigiert werden. Es ist auch möglich, die Fehlerkorrektur insgesamt als Quantenschaltkreis zu realisieren. Dazu wird abhängig vom Zustand des Syndromregisters $|\boldsymbol{c}\rangle$ eine Korrekturoperation auf dem Coderegister $|\boldsymbol{c}\rangle$ ausgeführt. Dieser Schaltkreis ist im allgemeinen aber sehr komplex, da er einer Tabellierung von Syndrom und Fehler entspricht und somit exponentiell viele Fälle unterschieden werden müssen.

5.2 Meggitt–Decodierer

Nachfolgend wird nun eine Methode vorgestellt, wie für zyklische Quantencodes die gesamte Fehlerkorrektur effizient als Quantenschaltkreis implementiert werden kann. Ausgangspunkt ist der sogenannte Meggitt–Decoder (cf. [MaSl77]) in Bild 4.

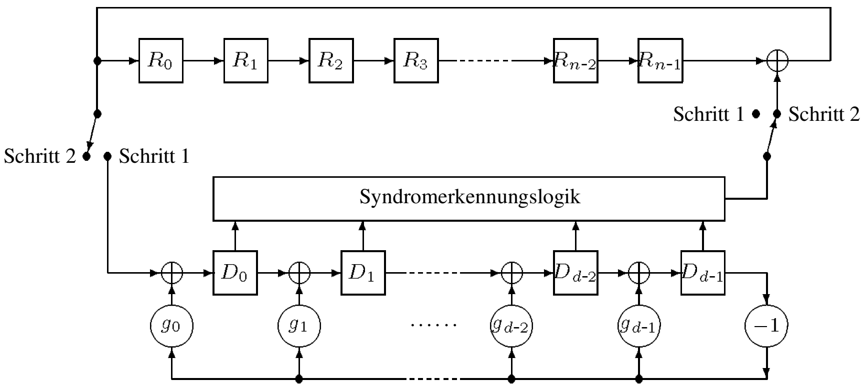
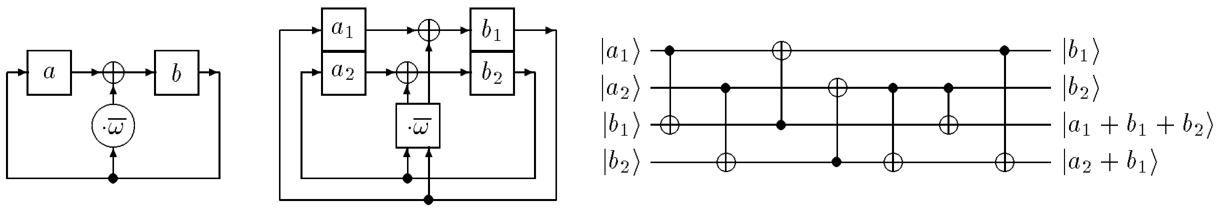


Bild 4: Schaltkreis zur Fehlerkorrektur nach Meggitt.

Dabei erfolgt in Schritt 1 die Syndromberechnung und in Schritt 2 die eigentliche Fehlerkorrektur. Die Syndromerkennungslogik muß nur Syndrome detektieren, die zu einem Fehler an der höchsten Stelle des Codes gehören. Diese werden dann korrigiert und das zu korrigierende Wort in den Registern R_i um eine Stelle zyklisch verschoben. Der Verschiebung des Syndroms in den Registern D_i erfolgt über ein rückgekoppeltes lineares Schieberegister, so daß das Syndrom entsprechend aktualisiert wird.

Für den Quantenschaltkreis wird nur Schritt 2 der Meggitt–Decodierung übertragen. Das Rückkoppelungspolynom für das Schieberegister ist $g(x) = x^2 + \overline{\varpi}\, x + 1$. Zunächst wird das Schieberegister über $GF(2)$ modelliert, dann kann es direkt in einen Quantenschaltkreis übersetzt werden (siehe Bild 5).



a) über $GF(4)$ b) über $GF(2)$ c) als Quantenschaltkreis

Bild 5: Schieberegister modulo $g(x) = x^2 + \overline{\varpi}\, x + 1$.

Der gesamte Quantenschaltkreis zur Korrektur der Fehler ist in Bild 6 wiedergegeben. Abhängig vom Syndrom werden zunächst Fehler in der ersten Postition c_1 des Codes korrigiert, was der Syndromerkennungslogik des Meggitt–Decoders entspricht. Anschließend wird das Syndrom zyklisch modulo $g(x)$ verschoben. Nun können mit fast dem gleichen Schaltkreis Fehler an der zweiten Stelle korrigiert werden. Würde wie beim Meggitt–Decoder auch das Codewort verschoben, so könnte in jedem Schritt genau dieselbe Korrekturoperation verwendet werden. Allerdings kann es relativ aufwendig sein, die Schiebeoperation im Quantenrechner zu implementieren.

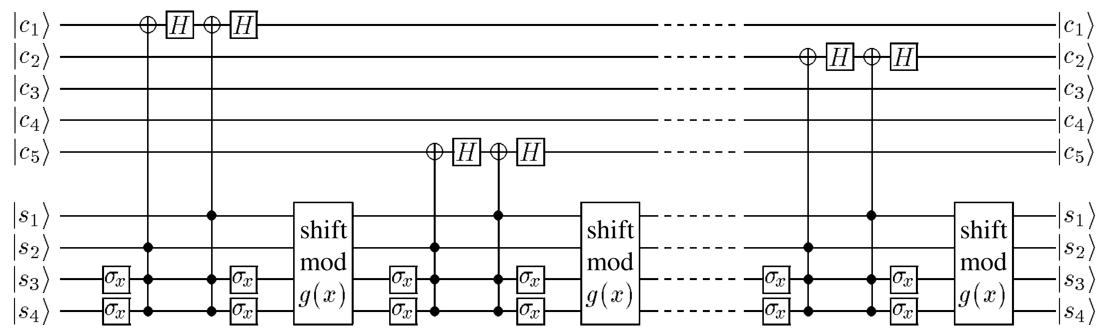


Bild 6: Schrittweise Korrektur der Fehler mit der (bis auf die zu korrigierende Position) gleichen Sequenz von Operationen in jedem Schritt bei gleichzeitiger zyklischen Verschiebung des Syndroms (analog zu Schritt 2 der Meggitt–Decodierung aus Bild 4).

Insgesamt zeigt sich, daß das Prinzip der Meggitt–Decodierung auf zyklische Quantencodes übertragbar ist. Wie schon bei diesem kleinen Beispiel ersichtlich ist, kann der resultierende Quantenschaltkreis modular aus ähnlichen Teilen aufgebaut werden. Im Gegensatz zu einem allgemeinen Decodierschaltkreis, bei dem für jeden Wert des Syndroms die zugehörige Korrekturoperation über bedingte Gatter realisert werden muß, sind auch die einzelnen Korrekturoperationen relativ einfach.

Literatur

[BBC95] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin und H. Weinfurter. „Elementary gates for quantum computation". *Physical Review A*, vol. 52, no. 5, November 1996, S. 3457–3467.

[BeGr96] Th. Beth und M. Grassl. „Improved Decoding of Quantum Error Correcting Codes from Classical Codes". In *Proceedings PhysComp96*, T. Toffoli, M. Biafore und J. Leao (Hrsg.). Boston, 24.–26. November 1996, S. 28–31.

[BeGr98] Th. Beth und M. Grassl. „The Quantum Hamming and Hexacodes". Erscheint in *Fortschritte der Physik*, Sonderausgabe zum Thema *Quantum Computing*.

[CRSS97] A. R. Calderbank, E. M. Rains, P. W. Shor, und N. J. A. Sloane. „Quantum Error Correction via Codes over $GF(4)$". In *Proceedings ISIT 97*, 1997, S. 292.

[Got96] D. Gottesman. „A Class of Quantum Error–Correcting Codes Saturating the Quantum Hamming Bound". *Physical Review A*, vol. 54, no. 3, September 1996, S. 1862–1868.

[GBP97] M. Grassl, Th. Beth und T. Pellizzari. „Codes for the Quantum Erasure Channel". *Physical Review A*, vol. 56, no. 1, Juli 1997, S. 33–38.

[Gro97] L. K. Grover. „Quantum Mechanics Helps in Searching for a Needle in a Haystack". *Physical Review Letters*, vol. 79, no. 2, 14. Juli 1997, S. 325–328.

[KBG98] A. Klappenecker, Th. Beth und M. Grassl. „Wavelettransformationen auf Quantenrechnern". Fachtagung Informations– und Mikrosystemtechnik, Magdeburg, 25.–27. März 1998 (in diesem Tagungsband).

[KnLa97] E. Knill und R. Laflamme. „A Theory of Quantum Error–Correcting Codes". *Physical Review A*, vol. 55, no. 2, Februar 1997, S. 900–911.

[LMPZ96] R. Laflamme, C. Miquel, J. P. Paz und W. H. Zurek. „Perfect Quantum Error Correction Code".*Physical Review Letters*, vol. 77, no. 1, Juli 1996, S. 198–201.

[Sho94] P. W. Shor. „Algorithms for Quantum Computation: Discrete Logarithmus and Factoring". In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, IEEE Computer Society Press. November 1994, S. 124–134.

[Sho95] P. W. Shor. „Scheme for reducing decoherence in quantum computer memory". *Physical Review A*, vol. 52, no. 4, Oktober 1995, S. R2493–R2496.

[MaSl77] F. J. MacWilliams und N. J. A. Sloane. *The Theory of Error–Correcting Codes.* Amsterdam: North–Holland, 1977.

[Ste96] A. Steane. „Multiple Particle Interference and Quantum Error Correction". *Proceedings Royal Society London A*, vol. 452, 1996, S. 2551–2577.

[Wer98] R. Werner. „Physikalische Grundlagen des Quantenrechners". Fachtagung Informations– und Mikrosystemtechnik, Magdeburg, 25.–27. März 1998 (in diesem Tagungsband).

[WoZu82] W. K. Wootters und W. H. Zurek. „A single quantum cannot be cloned". *Nature*, vol. 299, 1982, S. 802–803.