Wavelettransformationen auf Quantenrechnern

Andreas Klappenecker, Thomas Beth und Markus Grassl

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

In diesem Artikel wird erläutert, wie sich diskrete, periodisierte, unitäre Wavelettransformationen auf einem Quantenrechner effizient realisieren lassen. Insbesondere wird gezeigt, daß sich ein Elementarschritt der Wavelettransformation mit $O(kl)$ Elementargattern realisieren läßt, wobei l die Länge der verwendeten Waveletfilter und 2^k die Dimension des Berechnungsraumes $\ell^2(\mathbf{Z}/2^k\mathbf{Z})$ bezeichnet. Für eine Wavelettransformation $\ell^2(\mathbf{Z}/2^k\mathbf{Z}) \to \ell^2(\mathbf{Z}/2^k\mathbf{Z})$ ergibt sich somit ein Aufwand von höchstens $O(k^2 l)$ Elementargattern.

1. Einleitung

Das Interesse an Quantenrechnern ist in den letzten Jahren stark gestiegen, da sich bei gewissen Problemklassen ein (erhebliches) Potential zur Reduktion der Berechnungskomplexität durch die Nutzung quantenmechanischer Überlagerungs- und Verschränkungsprinzipen ergibt. In fast allen Quantenalgorithmen spielen Signaltransformationen eine ausgezeichnete Rolle. Beispielsweise ist die diskrete Fouriertransformation eine wesentliche Unterroutine im Faktorisierungsalgorithmus von Shor [8] und die Walsh-Hadamard-Transformation im Suchverfahren von Grover [4]. Høyer hat kürzlich weitere Signaltransformationen zur Verwendung auf Quantenrechnern vorgeschlagen [6], insbesondere zwei Wavelettransformationen. In diesem Artikel wird gezeigt, wie sich eine ganze Klasse von Wavelettransformationen effizient auf Quantenrechnern realisieren läßt.

2. Elementare Quantengatter

Der Zustand eines Quantenrechners läßt sich als Vektor im 2^k-dimensionalen Vektorraum $\mathbf{C}^{2^k}$ beschreiben. Wir schreiben die Standardbasis dieses Vektorraumes in der *ket*-Notation von Dirac, cf. [2]; die Basiselemente werden also mit $|\, x\rangle$ bezeichnet, wobei x ein Binärwort aus $\mathbf{F}_2^k$ ist. In dieser Notation läßt sich der Zustand eines Quantenbits beschreiben durch eine Linearkombination

$$a|\mathbf{0}\rangle + b|\mathbf{1}\rangle, \qquad \text{wobei} \quad a, b \in \mathbf{C}. \tag{1}$$

Häufig werden nur *normalisierte* Zustände betrachtet, die sich durch Vektoren mit Einheitslänge beschrieben lassen. Bei einem Quantenbit im normalisierten Zustand wird also verlangt, daß die Koeffizienten a, b in der Linearkombination (1) der Bedingung $|\, a\,|^2 + |\, b\,|^2 = 1$ genügen. Diese Normalisierung hat den sinnfälligen Grund, daß sich bei Messung des Zustandes (1) das Ergebnis 0 mit Wahrscheinlichkeit $|\, a\,|^2$ und das Ergebnis 1 mit Wahrscheinlichkeit $|\, b\,|^2$ ergibt.

In einem klassischen Rechner wird die Informationsverarbeitung durch logische Gatter realisiert. Diese Gatter finden auch beim Quantenrechner ihre Entsprechung, jedoch wird jedes Gatter durch eine unitäre Transformation realisiert.

Nicht-Gatter. Das Nicht-Gatter $U_{\mathtt{not}}$ operiert auf den Basiszuständen eines Quantenbits durch $U_{\mathtt{not}}|\,\mathbf{0}\rangle = |\,\mathbf{1}\rangle$ und $U_{\mathtt{not}}|\,\mathbf{1}\rangle = |\,\mathbf{0}\rangle$. Also gilt

$$U_{\mathtt{not}}(a|\,\mathbf{0}\rangle + b|\,\mathbf{1}\rangle) = a|\,\mathbf{1}\rangle + b|\,\mathbf{0}\rangle.$$

Ein-Bit-Gatter. Allgemeiner kann eine Operation U_M auf einem Quantenbit durch die Anwendung einer unitären 2×2-Matrix M beschrieben werden:

$$\left.\begin{array}{rcl} U_M|\,\mathbf{0}\rangle &=& m_{00}|\,\mathbf{0}\rangle + m_{01}|\,\mathbf{1}\rangle \\ U_M|\,\mathbf{1}\rangle &=& m_{10}|\,\mathbf{0}\rangle + m_{11}|\,\mathbf{1}\rangle \end{array}\right\}, \qquad \text{wobei} \qquad M = \begin{pmatrix} m_{00} & m_{01} \\ m_{10} & m_{11} \end{pmatrix}.$$

Im Falle des Nicht-Gatters wird also die Matrix M durch $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ gegeben.

Bedingtes Nicht. Wir können auf zwei Quantenbits die folgende Operation $U_{\mathtt{cnot}}$ durchführen:

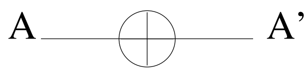
$$\begin{array}{rclcrcl} U_{\mathtt{cnot}}|\,\mathbf{00}\rangle &=& |\,\mathbf{00}\rangle, & \qquad & U_{\mathtt{cnot}}|\,\mathbf{01}\rangle &=& |\,\mathbf{11}\rangle, \\ U_{\mathtt{cnot}}|\,\mathbf{10}\rangle &=& |\,\mathbf{10}\rangle, & & U_{\mathtt{cnot}}|\,\mathbf{11}\rangle &=& |\,\mathbf{01}\rangle. \end{array}$$

Dieses Gatter führt genau dann eine Nicht-Operation auf dem höherwertigen Bit durch, wenn das niederwertige Bit im Zustand 1 ist.

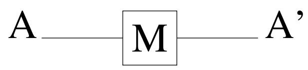
In völliger Analogie läßt sich ein bedingtes Nicht-Gatter $U_{\overline{\mathtt{c}}\mathtt{not}}$ formulieren, das genau dann eine Nicht-Operation auf dem höherwertigen Bit durchführt, wenn das niederwertige Bit im Zustand 0 ist:

$$\begin{array}{rclcrcl} U_{\overline{\mathtt{c}}\mathtt{not}}|\,\mathbf{00}\rangle &=& |\,\mathbf{10}\rangle, & \qquad & U_{\overline{\mathtt{c}}\mathtt{not}}|\,\mathbf{01}\rangle &=& |\,\mathbf{01}\rangle, \\ U_{\overline{\mathtt{c}}\mathtt{not}}|\,\mathbf{10}\rangle &=& |\,\mathbf{00}\rangle, & & U_{\overline{\mathtt{c}}\mathtt{not}}|\,\mathbf{11}\rangle &=& |\,\mathbf{11}\rangle. \end{array}$$

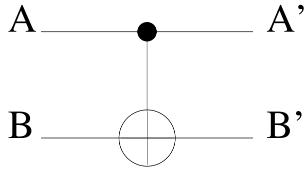
Feynman-Notation. Feynman hat eine bequeme Notation für diese Gatter eingeführt [3]; wir verwenden die notationelle Variante aus [1, 6]. Das Nicht-Gatter $U_{\mathtt{not}}$ mit Eingang A und Ausgang A' wird mit folgendem Symbol bezeichnet:



Das Gatter U_M mit Eingang A und Ausgang A' wird durch



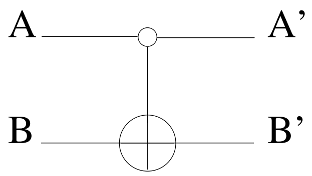
gekennzeichnet. Die eigentliche Stärke der Notation liegt in einer klaren Schreibweise für bedingte Gatter. Das Gatter $U_{\mathtt{cnot}}$ mit den Eingängen A und B wird durch



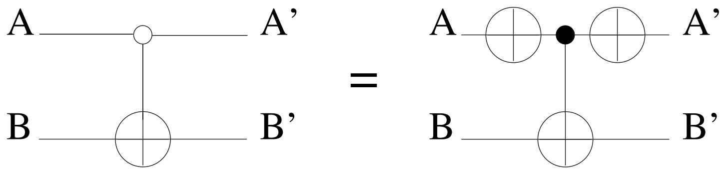
bezeichnet. Wenn am Eingang A eine 1 anliegt, dann wird eine Nicht-Operation auf B ausgeführt, ansonsten nur die Identität.

Die Gatter vom Typ $U_{\mathtt{cnot}}$ oder U_M nennen wir *elementare Quantengatter* oder einfach *elementare Gatter*. Es lassen sich alle unitären Operationen auf n Quantenbits durch eine Komposition dieser elementaren Gatter ausdrücken [1].

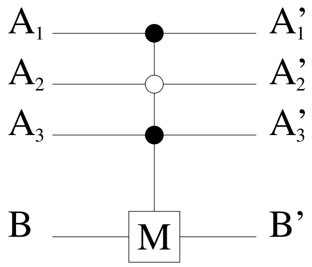
Für das Gatter $U_{\overline{\mathtt{c}}\mathtt{not}}$ wird die Notation



verwendet. Wenn am Eingang A eine 0 anliegt, dann wird eine Nicht-Operation auf B ausgeführt, ansonsten nur die Identität. Offensichtlich gilt



Allgemeiner können auch mehrere Bedingungen an die Ausführung eines Gatters geknüpft werden. Im folgenden Beispiel wird das Gatter U_M auf Eingang B dann und nur dann angewendet, wenn an den Eingängen A_1 und A_3 jeweils eine 1 und an Eingang A_2 eine 0 anliegt:



Tatsächlich lassen sich diese mehrfach bedingten Gatter mit geringem Aufwand aus elementaren Gattern aufbauen. In [1] wird gezeigt, daß lediglich $O(n)$ elementare Gatter notwendig sind, um ein n-fach bedingtes Gatter zu simulieren, das bei erfüllter Bedingung eine Operation vom Typ U_M auf einem Quantenbit durchführt. Der geringe Aufwand ergibt sich durch Hinzunahme eines weiteren Quantenbits als „Hilfsregister“. Wir gehen im folgenden davon aus, daß immer genügend Hilfsregister vorhanden sind.

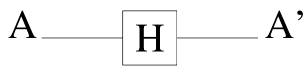
3. Haar-Transformationen

In diesem Abschnitt zeigen wir am Beispiel der Haar-Transformation, wie sich Waveletalgorithmen auf Quantennetzwerken realisieren lassen.

Für Signale der Länge 2 wird die Haar-Transformation durch die Hadamard-Matrix

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

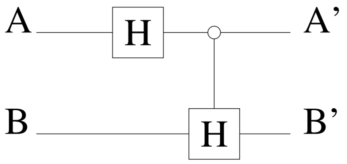
gegeben. Diese Transformation wird offensichtlich durch das Quantennetzwerk



realisiert. Für Signale der Länge 4 wird die Haar-Transformation durch die folgende Matrix gegeben:

$$\frac{1}{2} \begin{pmatrix} 1 & \sqrt{2} & 1 & 0 \\ 1 & -\sqrt{2} & 1 & 0 \\ 1 & 0 & -1 & \sqrt{2} \\ 1 & 0 & -1 & -\sqrt{2} \end{pmatrix} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & -1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & -1 \end{pmatrix} \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & \sqrt{2} & 0 & 0 \\ 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & \sqrt{2} \end{pmatrix}$$

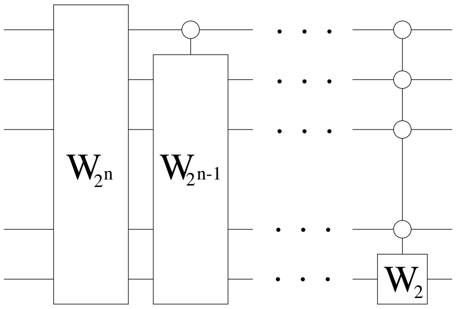
Die Faktorisierung der Matrix entspricht zwei Zerlegungsstufen im schnellen Algorithmus für die Wavelettransformation. Entsprechend dieser Faktorisierung läßt sich die Haar-Transformation der Länge 4 durch folgendes Quantennetzwerk realisieren:



Die Haar-Transformationen sind einfache Vertreter der Wavelettransformationen für Signale aus der Gruppenalgebra $\mathbf{C}[\mathbf{Z}/2^n\mathbf{Z}]$. Die Zerlegungsschritte sind angepaßt an die Untergruppenstruktur

$$\mathbf{Z}/2^n\mathbf{Z} \supset 2\mathbf{Z}/2^n\mathbf{Z} \supset 4\mathbf{Z}/2^n\mathbf{Z} \supset \cdots \supset 1.$$

Aufgrund der Schachtelung dieser Indexgruppen ergibt sich folgendes Grundprinzip für die Implementierung von Wavelettransformationen auf Quantenrechnern. Es sei mit $W_{2^k} \in U(2^k)$ die Transformationsmatrix eines Elementarschrittes der Waveletzerlegung bezeichnet. Dann läßt sich die zugehörige Wavelettransformation prinzipiell realisieren durch ein Netzwerk des folgenden Typs:



Es verbleibt zu zeigen, wie sich die Elementarschritte der Wavelettransformation realisieren lassen; dies ist das Ziel der folgenden Abschnitte. Zu diesem Zweck erinnern wir an eine Parameterisierung von „Quadrature Mirror Filter"-Paaren (kurz QMF-Paaren genannt) über $\ell^2(\mathbf{Z})$. Durch eine geeigenete Periodisierung dieser QMF-Paare erhalten wir – wie gewünscht – die Elementarschritte der Wavelettransformation über $\ell^2(\mathbf{Z}/2^n\mathbf{Z})$. Wir werden sehen, daß sich die Strukturinformation der Parameterisierung direkt in ein effizientes Quantennetzwerk übersetzen läßt.

4. Parameterisierung

Wir bezeichnen mit T_n den Verschiebungsoperator auf $\ell^2(\mathbf{Z})$, der durch $T_n\alpha(m) = \alpha(m-n)$ definiert ist. Weiter definieren wir einen Operator $O_W\colon \ell^2(\mathbf{Z}) \to \ell^2(\mathbf{Z})$ durch

$$\begin{array}{lcl} O_W\,\delta_{2n} & = & a\delta_{2n} + b\delta_{2n+1} \\ O_W\,\delta_{2n+1} & = & c\delta_{2n} + d\delta_{2n+1} \end{array} \quad \text{wobei} \quad W = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U(2).$$

Dieser Operator ist unitär. Bezeichnen wir mit $W^\dagger$ die konjugiert-komplexe transponierte Matrix von W, dann gilt $O_W^{-1} = O_{W^\dagger}$.

Definition 1 *Wir nennen $(\alpha, \beta) \in \ell^2(\mathbf{Z}) \times \ell^2(\mathbf{Z})$ genau dann ein QMF-Paar von $\ell^2(\mathbf{Z})$, wenn die Menge $\{T_{2k}\alpha, T_{2k}\beta \mid k \in \mathbf{Z}\}$ eine Orthonormalbasis von $\ell^2(\mathbf{Z})$ bildet.*

Eine Parameterisierung aller QMF-Paare ergibt sich aus folgendem Satz [5]:

Satz 2 (Holschneider, Pinkall) *Sei (α, β) ein QMF-Paar von $\ell^2(\mathbf{Z})$ mit*

$$\operatorname{supp}\alpha, \operatorname{supp}\beta \subset [0..2N-1].$$

Dann lassen sich α und β in der Form

$$\begin{aligned} \alpha &= O_{W_1} T_{-1} O_{W_2} \cdots T_{-1} O_{W_N} \delta_0 \\ \beta &= O_{W_1} T_{-1} O_{W_2} \cdots T_{-1} O_{W_N} \delta_1 \end{aligned}$$

ausdrücken, wobei $W_i \in SU(2)$ für $i > 1$ und $W_1 \in U(2)$.

Beweis Wir führen den Beweis per Induktion über N. Wir zeigen, daß α und β durch Anwenden der Operatoren O_W und T_{-1} auf δ_0 und δ_1 abgebildet werden können. Durch Invertierung aller Operationen ergibt sich dann die Aussage.

Im Fall $N = 1$ bilden die Vektoren $a := (\alpha(0), \alpha(1))$ und $b := (\beta(0), \beta(1))$ eine Orthogonalbasis von $\mathbf{C}^2$. Es gibt somit eine Matrix $W_1 \in U(2)$, so daß $aW_1 = (1, 0)$ und $bW_1 = (0, 1)$ gilt. Nach Definition folgt $O_{W_1}\alpha = \delta_0$ und $O_{W_1}\beta = \delta_1$.

Im Fall $N > 1$ gilt

$$\langle \alpha \mid T_{2(N-1)}\alpha \rangle = \langle \beta \mid T_{2(N-1)}\beta \rangle = \langle \alpha \mid T_{2(N-1)}\beta \rangle = \langle \beta \mid T_{2(N-1)}\alpha \rangle = 0.$$

Hieraus ergibt sich, daß die folgenden Vektoren aus $\mathbf{C}^2$ paarweise orthogonal sind:

$$\begin{aligned} a_l &:= (\alpha(0), \alpha(1)), \qquad & a_r &:= (\alpha(2N-2), \alpha(2N-1)), \\ b_l &:= (\beta(0), \beta(1)), \qquad & b_r &:= (\beta(2N-2), \beta(2N-1)). \end{aligned}$$

Es gibt somit eine Matrix $W_N \in SU(2)$, so daß

$$\langle a_l W_N \mid (1,0) \rangle = \langle b_l W_N \mid (1,0) \rangle = \langle a_r W_N \mid (0,1) \rangle = \langle b_r W_N \mid (0,1) \rangle = 0$$

Als Konsequenz ergibt sich, daß $\operatorname{supp} O_{W_N}\alpha$ und $\operatorname{supp} O_{W_N}\beta$ in $[1..2N-2]$ enthalten sind. Somit ist der Träger der Folge $T_1 O_{W_N}\alpha$ und der Folge $T_1 O_{W_N}\beta$ in $[0..2(N-1)-1]$ enthalten. □

5. Periodisierung

Wir bezeichnen mit $\overline{T}_n$ den Verschiebungsoperator auf $\ell^2(\mathbf{Z}/N\mathbf{Z})$, der durch $\overline{T}_n\alpha(k) = \alpha(k - n \bmod N)$ definiert wird. Weiter definieren wir einen Operator $\overline{O}_W$ auf $\ell^2(\mathbf{Z}/2N\mathbf{Z})$ durch

$$\begin{aligned} \overline{O}_W\, \delta_{2n} &= a\delta_{2n} + b\delta_{2n+1} \\ \overline{O}_W\, \delta_{2n+1} &= c\delta_{2n} + d\delta_{2n+1} \end{aligned} \quad \text{wobei} \quad W = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in U(2).$$

In Analogie zum vorigen Abschnitt vereinbaren wir folgende Sprechweise:

Definition 3 *Wir nennen (α, β) genau dann ein QMF-Paar von $\ell^2(\mathbf{Z}/2N\mathbf{Z})$, wenn die Menge $\{\overline{T}_{2k}\alpha, \overline{T}_{2k}\beta \mid k \in [0..N-1]\}$ eine Orthonormalbasis von $\ell^2(\mathbf{Z}/2N\mathbf{Z})$ bildet.*

Eine Methode zur Gewinnung von neuen QMF-Paaren aus einem gegebenen QMF-Paar geben wir in folgendem Lemma an:

Lemma 4 *Sei (α, β) ein QMF-Paar von $\ell^2(\mathbf{Z}/2N\mathbf{Z})$, und mit O sei ein unitärer Operator auf $\ell^2(\mathbf{Z}/2N\mathbf{Z})$ bezeichnet, der mit T_2 kommutiert. Dann ist $(O\alpha, O\beta)$ ebenfalls ein QMF-Paar von $\ell^2(\mathbf{Z}/2N\mathbf{Z})$. Insbesondere sind $(\overline{T}_k\alpha, \overline{T}_k\beta)$ und $(\overline{O}_W\alpha, \overline{O}_W\beta)$ wieder QMF-Paare.*

Beweis Ein unitärer Operator bildet eine Orthonormalbasis wieder auf eine Orthonormalbasis ab. Somit ist $B := \{O\overline{T}_{2k}\alpha, O\overline{T}_{2k}\beta \,|\, k \in [0..N-1]\}$ eine Orthonormalbasis. Da O mit $\overline{T}_2$ kommutiert, läßt sich die Menge B in der Form $B = \{\overline{T}_{2k}O\alpha, \overline{T}_{2k}O\beta \,|\, k \in [0..N-1]\}$ schreiben. Die Operatoren T_k und O_W kommutieren offensichtlich mit T_2, womit die Behauptung gezeigt ist. □

Wir definieren einen *Periodisierungsoperators* Π_N durch

$$\Pi_N\colon \ell^2(\mathbf{Z}) \longrightarrow \ell^2(\mathbf{Z}/N\mathbf{Z}), \quad \alpha(k) \longmapsto \sum_{m\in\mathbf{Z}} \alpha(k-mN).$$

Lemma 5 *Es gelten die Relationen*

$$\Pi_N\, T_n = \overline{T}_{n \bmod N}\, \Pi_N \qquad \textit{und} \qquad \Pi_{2N}\, O_W = \overline{O}_W\, \Pi_{2N}.$$

Beweis Die Behauptung ergibt sich als direkte Konsequenz aus den Definitionen der Operatoren. □

Satz 6 *Sei* (α, β) *ein QMF-Paar von* $\ell^2(\mathbf{Z})$ *mit* $\operatorname{supp}\alpha, \operatorname{supp}\beta \subset [0..2N-1]$. *Das periodisierte Paar* $(\Pi_{2M}\alpha, \Pi_{2M}\beta)$ *ist ein QMF-Paar von* $\ell^2(\mathbf{Z}/2M\mathbf{Z})$ *und läßt sich in der Form*

$$\begin{aligned}\Pi_{2M}\alpha &= \overline{O}_{W_1}\overline{T}_{-1}\overline{O}_{W_2}\cdots\overline{T}_{-1}\overline{O}_{W_N}\delta_0\\ \Pi_{2M}\beta &= \overline{O}_{W_1}\overline{T}_{-1}\overline{O}_{W_2}\cdots\overline{T}_{-1}\overline{O}_{W_N}\delta_1\end{aligned}$$

ausdrücken, wobei $W_i \in SU(2)$ *für* $i > 1$ *und* $W_1 \in U(2)$.

Beweis Nach Satz 2 läßt sich (α, β) in der Form

$$\begin{aligned}\alpha &= O_{W_1}T_{-1}O_{W_2}\cdots T_{-1}O_{W_N}\delta_0\\ \beta &= O_{W_1}T_{-1}O_{W_2}\cdots T_{-1}O_{W_N}\delta_1\end{aligned}$$

ausdrücken. Für das periodisierte Paar $(\Pi_{2M}\alpha, \Pi_{2M}\beta)$ ergibt sich unter Verwendung von Lemma 5:

$$\begin{aligned}\Pi_{2M}\alpha &= \Pi_{2M}O_{W_1}T_{-1}O_{W_2}\cdots T_{-1}O_{W_N}\delta_0 &= \overline{O}_{W_1}\overline{T}_{-1}\overline{O}_{W_2}\cdots\overline{T}_{-1}\overline{O}_{W_N}\delta_0\\ \Pi_{2M}\beta &= \Pi_{2M}O_{W_1}T_{-1}O_{W_2}\cdots T_{-1}O_{W_N}\delta_1 &= \overline{O}_{W_1}\overline{T}_{-1}\overline{O}_{W_2}\cdots\overline{T}_{-1}\overline{O}_{W_N}\delta_1\end{aligned}$$

Also ist $(\Pi_{2M}\alpha, \Pi_{2M}\beta)$ von der gewünschten Form; insbesondere ist dieses Paar nach Lemma 4 ein QMF-Paar. □

6. Realisierung der Elementarschritte

In diesem Abschnitt zeigen wir, wie sich ein Elementarschritt der diskreten Wavelettransformation für periodisierte QMF-Paare effizient realisieren läßt.

Ein Syntheseschritt mit QMF-Paar $(\Pi_{2M}\alpha, \Pi_{2M}\beta)$ läßt sich in der Notation von Satz 6 beschreiben durch den Operator:

$$\overline{O}_{W_1}\overline{T}_{-1}\overline{O}_{W_2}\cdots\overline{T}_{-1}\overline{O}_{W_N}.$$

Daher kann der zugehörige Analyseschritt beschrieben werden durch den inversen Operator

$$\overline{O}_{W_N^\dagger}\overline{T}_1\cdots\overline{O}_{W_2^\dagger}\overline{T}_1\overline{O}_{W_1^\dagger}.$$

Ein Elementarschritt kann daher mit Hilfe der Operatoren $\overline{T}_1$ und $\overline{O}_W$ realisiert werden. Bezüglich der Standardbasis von $\ell^2(\mathbf{Z}/2M\mathbf{Z})$ läßt sich der Operator $\overline{T}_1$ ausdrücken durch die Matrix $S := (\delta_{i-1 \bmod 2M, j})_{i,j\in[0..2M-1]}$ und der Operator $\overline{O}_W$ durch die Matrix $I \otimes W$.

Beispiel 7 Es bezeichne $R(\theta)$ die Rotationsmatrix

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}.$$

Ein Zerlegungsschritt bezüglich des Daubechies-Filters der Ordnung 2 für Signale aus $\ell^2(\mathbf{Z}/8\mathbf{Z})$ läßt sich beschreiben durch den Operator $\overline{O}_{R(7\pi/12)}\overline{T}_1\overline{O}_{R(5\pi/6)}$ oder alternativ durch die Matrix

$$(I_4 \otimes R(5\pi/6))\, S\, (I_4 \otimes R(7\pi/12)).$$

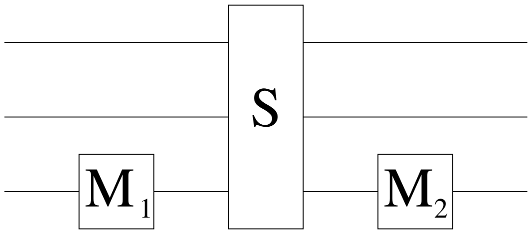
Ausmultiplizieren dieser Matrizen ergibt:

$$\begin{pmatrix}
h_3 & h_0 & 0 & 0 & 0 & 0 & h_1 & h_2 \\
h_2 & -h_1 & 0 & 0 & 0 & 0 & h_0 & -h_3 \\
h_1 & h_2 & h_3 & h_0 & 0 & 0 & 0 & 0 \\
h_0 & -h_3 & h_2 & -h_1 & 0 & 0 & 0 & 0 \\
0 & 0 & h_1 & h_2 & h_3 & h_0 & 0 & 0 \\
0 & 0 & h_0 & -h_3 & h_2 & -h_1 & 0 & 0 \\
0 & 0 & 0 & 0 & h_1 & h_2 & h_3 & h_0 \\
0 & 0 & 0 & 0 & h_0 & -h_3 & h_2 & -h_1
\end{pmatrix}$$

wobei

$$h_0 := \frac{1+\sqrt{3}}{4\sqrt{2}}, \quad h_1 := \frac{3+\sqrt{3}}{4\sqrt{2}}, \quad h_2 := \frac{3-\sqrt{3}}{4\sqrt{2}}, \quad h_3 := \frac{1-\sqrt{3}}{4\sqrt{2}}.$$

Realisiert wird dies durch das Gatternetzwerk



wobei $M_1 := R(5\pi/6)$ und $M_2 := R(7\pi/12)$. □

Satz 8 *Sei (α, β) ein QMF-Paar von $\ell^2(\mathbf{Z})$ mit* $\operatorname{supp}\alpha, \operatorname{supp}\beta \subset [0..2N-1]$ *und* $(\Pi_{2^n}\alpha, \Pi_{2^n}\beta)$ *das zugehörige periodisierte QMF-Paar von $\ell^2(\mathbf{Z}/2^n\mathbf{Z})$. Dann läßt sich ein (bedingter) elementarer Zerlegungsschritt mit $O(nN)$ Elementargattern realisieren.*

Beweis Aus Satz 6 folgt, daß lediglich N Operatoren vom Typ $\overline{O}_W$ und $N-1$ Operatoren vom Typ $\overline{T}_1$ zur Realisierung des Elementarschrittes notwendig sind. Es wurde in [9] gezeigt, daß sich die (bedingte) Addition modulo 2^n mit $O(n)$ Elementargatter aufbauen läßt, wenn genügend Hilfsregister vorhanden sind. Dies ergibt einen Gesamtaufwand von höchstens $O(nN)$ Gattern. □

Korollar 9 *Sei (α, β) wie im vorigen Satz gegeben. Eine Wavelettransformation auf $\ell^2(\mathbf{Z}/2^n\mathbf{Z})$, die in jedem Elementarschritt eine periodisierte Version von (α, β) benutzt, läßt sich aus höchstens $O(Nn^2)$ Elementargattern aufbauen.*

Dank. Andreas Klappenecker dankt der Deutschen Forschungsgemeinschaft für die Unterstützung durch den Sonderforschungsbereich SFB 414.

Literatur

[1] 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*, 52(5):3457–3467, 1995.

[2] P. A. M. Dirac. *The Principles of Quantum Mechanics*. Oxford University Press, 3. Auflage, 1949.

[3] R. P. Feynman. *Feynman Lectures on Computation*. Addison-Wesley, 1996.

[4] L. K. Grover. Quantum Mechanics Helps in Searching for a Needle in a Haystack. *Physical Review Letters*, 79(2):325–328, 1997.

[5] M. Holschneider und U. Pinkall. Quadratic Mirror Filters and Loop Groups. Preprint, TU-Berlin, 1993.

[6] P. Høyer. Efficient quantum transforms. LANL preprint quant–ph/9702028, Feb. 1997.

[7] A. Klappenecker. Algebraische Wavelets. (In Vorbereitung), Universität Karlsruhe, 1998.

[8] Peter W. Shor. Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms. In *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, November 1994.

[9] V. Vedral, A. Barenco und A. Ekert. Quantum networks for elementary arithmetic operations. *Phys. Rev. A*, 54:147–153, 1996.