Quantenfouriertransformation

In diesem Kapitel behandeln wir die Fouriertransformation auf endlichen abelschen Gruppen und effiziente klassiche und Quantenalgorithmen zur Berechnung von Fouriertransformierten, im Hinblick auf die Quantenalgorithmen zum Faktorisieren und zum diskreten Logarithmus.

Fourieranalyse auf endlichen abelschen Gruppen

Fouriertransformationen betrachtet man üblicherweise für Mengen $Z(G)$ von Funktionen $f : G \to \mathbb{C}$ auf einem Definitionsbereich G, welche mit der punktweisen Addition von Funktionen und punktweisen Multiplikation von Elementen aus $\mathbb{C}$ mit Funktionen und bezüglich eines (hermiteschen) Skalarprodukt $\langle \cdot, \cdot \rangle$ die Struktur von Hilberträumen tragen. Mit einem Orthonormalsystem von Funktionen $\chi_i : G \to \mathbb{C}$ aus Z und i aus einer geeigneten Indexmenge I kann man dann $f = \sum_{i \in I} \langle f, \chi_i \rangle \chi_i$ schreiben. Die $\langle f, \chi_i \rangle$ sind hierbei die Fourierkoeffizienten von f, die Abbildung $F(f) : i \mapsto \langle f, \chi_i \rangle$ die Fouriertransformierte von f, und schließlich $F : f \mapsto F(f)$ die Fouriertransformation.

Häufig betrachtet man $G = \mathbb{R}$. Diese Situation kann diskretisiert werden, indem man diskrete Teilmengen oder ausreichend große, endliche Mengen $G \subseteq \mathbb{R}$ betrachtet. Man spricht dann von diskreter Fouriertransformation.

Wir interessieren uns für den Fall, daß G eine endliche abelsche Gruppe ist, und sprechen von Fouriertransformation auf endlichen abelschen Gruppen. Thematisch gehört dies in die Darstellungstheorie endlicher Gruppen, auf die wir hier aber nicht weiter eingehen werden.

Sei G von nun an eine endliche, abelsche Gruppe. Die zu G duale Gruppe $\hat{G}$ wird als $\mathrm{Hom}(G, \mathbb{C}^\times)$ definert, der Gruppe aller Homomorphismen von G nach $\mathbb{C}^\times$. Das Gruppengesetz ist hier durch punktweise Multiplikation definert. Die Elemente der Gruppe $\hat{G}$ heißen Charaktere von G, und $\hat{G}$ wird daher auch Charaktergruppe von G genannt. Die duale Gruppe $\hat{G}$ ist offenbar wieder abelsch. Für $\chi \in \hat{G}$ und $g \in G$ gilt $\chi(g)^{\#G} = \chi(g^{\#G}) = \chi(1) = 1$, $\chi(g)$ ist also eine $\#G$-te Einheitswurzel der Form $\exp(2\pi i a/\#G)$ mit $0 \leq a \leq \#G - 1$. Somit $\mathrm{im}(\chi) \subseteq \mu_{\#G}$, wobei $\mu_n \subseteq \mathbb{C}^\times$ die zyklische Gruppe der n-ten Einheitswurzeln in $\mathbb{C}$ bezeichnet.

Ist $f \in \mathrm{Hom}(G, H)$, so erhalten wir durch Zurückziehung entlang f den dualen Homomorphismus $\hat{f} \in \mathrm{Hom}(\hat{H}, \hat{G})$. Dies macht $\hat{\cdot} = \mathrm{Hom}(\cdot, \mathbb{C}^\times)$ in einen kontravarianten Funktor.

1 Satz. *Für eine endliche abelsche Gruppe G gelten:*

(i) *$\hat{G} \cong G$, wobei die Isomorphie nicht natürlich gegeben ist (sondern von der Wahl von Erzeugern abhängt).*

(ii) *Die Homomorphismus $G \to (\hat{G})^\wedge$ mit $g \mapsto h_g$, wobei h_g durch $h_g(\chi) = \chi(g)$ für $\chi \in \hat{G}$ definert ist, ist ein natürlicher Isomorphismus.*

(iii) *Sei $\mathcal{C}$ die Kategorie der endlichen, abelschen Gruppen. Der Funktor $\mathrm{Hom}(\cdot, \mathbb{C}^\times) : \mathcal{C}^{opp} \to \mathcal{C}$ ist voll, treu und exakt.*

Beweis. (i): Dies folgt aus zwei Beobachtungen: Die erste Beobachtung ist, daß die Aussage für zyklische Gruppen G gilt, weil dann $\hat{G}$ ebenfalls zyklisch von der Ordnung $\#G$ ist. Dies wiederum führt sich auf die Tatsache zurück, daß die $\#G$-ten Einheitswurzeln in $\mathbb{C}^\times$ eine zyklische Gruppe der Ordnung $\#G$ bilden und weil allgemein $\mathrm{Hom}(\mathbb{Z}/n\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}) \cong \mathbb{Z}/n\mathbb{Z}$ gilt. Die zweite Beobachtung ist, daß $\mathrm{Hom}(\cdot, \mathbb{C}^\times)$ direkte Summen in direkte Produkte überführt, woraus die Aussage für allgemeines G durch Zerlegung von G als endliche direkte Summe zyklischer Untergruppen folgt.

(ii): Der Homomorphismus ist injektiv, denn gäbe es ein $g \neq 1$ mit $\chi(g) = 1$ für alle χ, so wäre der Zurückziehungshomomorphismus $\mathrm{Hom}(G/H, \mathbb{C}^\times) \to \mathrm{Hom}(G, \mathbb{C}^\times)$ für $H = \langle g \rangle$ ein Isomorphismus, was nach (i) aus Anzahlgründen nicht sein kann. Ebenfalls aus Anzahlgründen ist der Homomorphismus dann auch surjektiv.

(iii): Ohne Beweis (voll und treu folgen aus (ii), exakt folgt, da $\mathbb{C}^\times$ injektiv ist, da $\mathbb{C}^\times$ divisibel ist). Voll und treu heißen, daß unter $\hat{\cdot}$ die Isomorphie $\mathrm{Hom}(G, H) \cong \mathrm{Hom}(\hat{H}, \hat{G})$ besteht. Exakt heißt, daß für eine Untergruppe $H \subseteq G$ bezüglich der Zurückziehungseinbettung $\widehat{(G/H)} \subseteq \hat{G}$ und Zurückziehungseinschränkung die Isomorphie $\hat{H} \cong \hat{G}/\widehat{(G/H)}$ besteht. $\square$

Wir kommen nun zu den zu betrachtenden Funktionenräumen. Mit

$$Z(G) = \{f \mid f : G \to \mathbb{C}\}$$

bezeichnen wir den Vektorraum über $\mathbb{C}$ aller Funktionen von G nach $\mathbb{C}$, mit $(f+g)(x) := f(x) + g(x)$ und $(cf)(x) := cf(x)$, zusammen mit der symmetrischen Bilinearform

$$\langle f, h\rangle_G = (1/\#G)^{-1/2} \sum_{g\in G} f(g)h(g^{-1})$$

und dem hermiteschen Skalarprodukt

$$\langle f, h\rangle = \sum_{g\in G} f(g)\overline{h(g)}.$$

Die Elemente dieses Vektorraums sind im wesentlichen nichts anderes als Elemente in $\mathbb{C}^{\#G}$, wenn die Koordinaten mit $g \in G$ durchnumeriert werden. Die Gruppenstruktur erlaubt zusätzlich, auf den Koordinaten Rechnungen durchzuführen. Die Elemente aus $Z(G)$ werden auch Klassenfunktionen genannt (im nicht-abelschen Fall sind es Funktionen auf Konjugationsklassen von G nach $\mathbb{C}$).

Als Mengen gilt $\hat{G} \subseteq Z(G)$. Der folgende Satz zeigt, daß die Elemente von $\hat{G}$ eine Orthogonalbasis ähnlich den obigen χ_i liefern.

2 Satz. *Die Bilinearform $\langle\cdot,\cdot\rangle_G$ ist nicht ausgeartet. Für $\chi, \psi \in \hat{G}$ gilt*

$$\langle \chi, \psi\rangle_G = \begin{cases} (\#G)^{1/2} & \textit{für } \chi = \psi, \\ 0 & \textit{sonst.} \end{cases}$$

Die Charaktere aus $\hat{G}$ bilden bezüglich $\langle\cdot,\cdot\rangle_G$ eine Orthogonalbasis von $Z(G)$.

Beweis. Für $g \in G$ sei $e_g : G \to \mathbb{C}$ mit $e_g(h) = \delta_{g,h}$ (die e_g bilden nebenbei eine Basis von $Z(G)$). Ist $f \in Z(G)$ und $f \neq 0$, so gibt es ein $g \in G$ mit $f(g^{-1}) \neq 0$. Dann gilt $\langle e_g, f\rangle_G = (1/\#G)^{-1/2} f(g^{-1}) \neq 0$, folglich ist $\langle\cdot,\cdot\rangle_G$ nicht ausgeartet. Diese Aussage folgt aber auch aus den beiden anderen Aussagen.

Für die zweite Aussage zeigen wir zunächst $\sum_{g\in G} \chi(g) = \#G \cdot \delta_{\chi,1}$. Es gilt $\mathrm{im}(\chi) = \mu_\ell$ für ein $\ell \in \mathbb{Z}^{\geq 1}$. In $t^\ell - 1 = \prod_{x\in\mu_\ell}(t-x)$ ist der Spurkoeffizient für $\ell > 1$ gleich Null und für $\ell = 1$ gleich eins, also $\sum_{x\in\mu_\ell} x = \delta_{\ell,1}$. Jedes $x \in \mu_\ell$ tritt genau $\#\ker(\chi)$ mal als Summand in $\sum_{g\in G}\chi(g)$ auf. Damit folgt $\sum_{g\in G}\chi(g) = \#\ker(\chi)\cdot\delta_{\ell,1} = \#G\cdot\delta_{\chi,1}$. Wenden wir die erhaltene Gleichung auf den Charakter $\chi\psi^{-1}$ an, ergibt sich $\sum_{g\in G}(\chi\psi^{-1})(g) = \sum_{g\in G}\chi(g)\psi(g^{-1}) = \#G\cdot\delta_{\chi,\psi}$ und daraus die zweite Aussage.

Nach der zweiten Aussage gilt $\langle\sum_\chi \lambda_\chi\chi, \psi\rangle_G = \lambda_\chi(\#G)^{1/2}\delta_{\chi,\psi}$, folglich ist die Linearkombination $\sum_\chi \lambda_\chi\chi = 0$ genau dann, wenn alle $\lambda_\chi = 0$ sind. Daher sind die Charaktere aus $\hat{G}$ linear unabhängig. Aus Dimensionsgründen sind sie dann nach Satz 1, (i) auch eine Basis. $\square$

3 Korollar. *Es gelten die Orthogonalitätsrelationen*

$$\sum_{g\in G}\chi(g)\psi(g^{-1}) = \#G\cdot\delta_{\chi,\psi}\qquad \textit{für } \chi,\psi\in\hat{G}$$

und

$$\sum_{\chi\in\hat{G}}\chi(g)\chi(h)^{-1} = \#G\cdot\delta_{g,h}\qquad \textit{für } g,h\in G.$$

Beweis. Die erste Aussage ist die Gleichung im Satz 2, und die zweite folgt aus der ersten Aussage angewandt auf $\hat{G}$ und aus Satz 1, (*ii*). □

Häufige Spezialfälle ergeben sich, wenn man $\psi = 1$ oder $h = 1$ verwendet.

Die Fouriertransformation wird nun durch

$$F_G : Z(G)\to Z(\hat{G}),\quad F_G(f):\chi\mapsto\langle f,\chi\rangle_G$$

gegeben. Es ist klar, daß F_G eine lineare Abbildung ist. Die im Beweis von Satz 2 für $g\in G$ definierten Funktionen e_g bilden eine Basis von $Z(G)$, und ebenso bilden die e_χ für $\chi\in\hat{G}$ eine Basis von $Z(\hat{G})$. Für $f\in Z(G)$ gilt dann $f = \sum_{g\in G} f(g)e_g$ und

$$\begin{aligned}F_G(f) &= \sum_{\chi\in\hat{G}} F_G(f)(\chi)e_\chi = \sum_{\chi\in\hat{G}}\langle f,\chi\rangle_G e_\chi\\ &= \sum_{\chi\in\hat{G}}\sum_{g\in G} f(g)\langle e_g,\chi\rangle_G e_\chi = (\#G)^{-1/2}\sum_{\chi\in\hat{G}}\sum_{g\in G} f(g)\chi(g^{-1})e_\chi.\end{aligned}$$

Bezüglich der Basen e_g und e_χ wird F also durch die $\#G\times\#G$ Matrix

$$M_G = (\#G)^{-1/2}\left(\chi(g^{-1})\right)_{\chi,g}$$

dargestellt. Im folgenden identifizieren wir $(\hat{G})^\wedge$ mit G wie in Satz 1, (*ii*) und fassen also insbesondere Elemente aus G auch als Elemente aus $(\hat{G})^\wedge$ auf. Damit wird $F_{\hat{G}}$ zu einer linearen Abbildung $Z(\hat{G})\to Z(G)$ mit

$$M_{\hat{G}} = (\#G)^{-1/2}\left(g(\chi^{-1})\right)_{g,\chi} = (\#G)^{-1/2}\left(\chi(g^{-1})\right)_{g,\chi} = M_G^t.$$

4 Satz. *Die Fouriertransformation besitzt folgende zwei Eigenschaften:*

(i) *Es gilt* $F_{\hat{G}}(F_G(f))(g) = f(g^{-1})$ *für alle* $g\in G$.

(ii) *Die Matrix* M_G *is unitär.*

Beweis. Es gilt $F_{\hat{G}}(F_G(f)) : g \mapsto \langle F_G(f), g\rangle_G$. Damit ergibt sich

$$\begin{aligned}\langle F_G(f), g\rangle_G &= (\#G)^{-1/2} \sum_{\chi} F_G(f)(\chi)\chi(g)^{-1} = (\#G)^{-1/2} \sum_{\chi} \langle f, \chi\rangle_G \chi(g)^{-1} \\ &= (\#G)^{-1} \sum_{\chi,h} f(h)\chi(h^{-1})\chi(g)^{-1} \\ &= (\#G)^{-1} \sum_{h} f(h) \sum_{\chi} \chi(h^{-1})h(g)^{-1} \\ &= \sum_{h} f(h)\delta_{h,g^{-1}} = f(g^{-1}),\end{aligned}$$

was (i) beweist (wir hätten auch $M_{\hat{G}}M_G$ berechnen können, was die umgekehrte Einheitsmatrix liefert). Für Aussage (ii) bemerken wir, daß die zu M_G adjungierte Matrix $M_G^* = (\#G)^{-1/2}(\chi(g))_{g,\chi}$ ist, unter Verwendung von $\overline{\chi(g)} = \chi(g)^{-1} = \chi(g^{-1})$. Nach den Orthogonalitätsrelationen gilt $M_F M_F^* = M_F^* M_F = 1$. □

Darstellung auf einem Quantencomputer

Bevor wir mit der Fouriertransformation fortfahren, betrachten wir, wie Elemente aus $Z(G)$ in einem Quantencomputer dargestellt werden können.

Wir nehmen an, daß die Elemente in G durch Bitstrings der Länge n eindeutig beschrieben werden können, daß wir also eine injektive (in beiden Richtungen effizient berechenbare) Codierungsabbildung $\iota : G \to \{0,1\}^n$ haben. Es gilt offenbar notwendigerweise $\#G \leq 2^n$. Wir können dann jedes $g \in G$ durch den Zustand $|\iota(g)\rangle$ beschreiben, und jedes $f \in Z(G)$ durch die noch geeignet zu normierende Superposition $\sum_{g\in G} f(g)|\iota(g)\rangle$. Während g durch $|\iota(g)\rangle$ wirklich bestimmt wird, gilt dies für f und $\sum_{g\in G} f(g)|\iota(g)\rangle$ nicht. Wir erhalten Information nämlich nur nach Messungen, welche uns in ersterem Fall stets $|\iota(g)\rangle$, in letzterem Fall aber nur ein zufälliges $|\iota(g)\rangle$ liefert. In den angestrebten Anwendungen geht es auch nicht darum, f genau darzustellen, sondern die auftretenden Wahrscheinlichkeiten so zu transformieren, daß man einen gesuchten Zielwert $|\iota(g)\rangle$ mit hoher Wahrscheinlichkeit erhält. Die Transformationen müssen dabei natürlich dergestalt sein, daß die Messung nicht $|x\rangle$ mit $x \notin \mathrm{im}(\iota)$ liefert.

Die Eigenschaft, daß Registerzustände als Tensorprodukte einfacherer Zustände geschrieben werden können, hat hier im allgemeinen keine algebraische Bedeutung in $Z(G)$. In speziellen Fällen kann man $Z(G)$ aber als Tensorprodukt auffassen, und möchte dies auch mit einer Tensorproduktzerlegung für die Registerzustände in Einklang bringen. Sei $H \subseteq G$ eine Untergruppe und $r_{G,H} : G/H \to G$ eine Repräsentantenfunktion mit $r_{G,H}(H) = 1$ (es gilt also $r_{G,H}(gH)H = gH$ für alle $g \in G$). Wir betrachten im folgenden ausschließlich Repräsentantenfunktionen, welche diese Eigenschaft haben. Mit Hilfe von $r_{G,H}$ erhalten wir einen Isomorphismus

$$i_{G,H} : Z(G/H) \otimes Z(H) \to Z(G),$$

welcher durch $f \otimes h \mapsto g_{f,h}$ mit $g_{f,h}(r_{G,H}(x)y) = f(x)h(y)$ für $x \in G/H$ und $y \in H$ definiert ist. Hierbei durchläuft $r_{G,H}(x)y$ alle Werte aus G. Für die speziellen Klassenfunktionen e_x, e_y ergibt sich

$$e_x \otimes e_y \mapsto e_{r_{G,H}(x)y}.$$

Für die umgekehrte Richtung des Isomorphismus zerlegen wir $z \in G$ eindeutig in der Form $z = r_{G,H}(x)y$ mittels $x = zH \in G/H$ und $y = z/r_{G,H}(x) \in H$. Dann gilt $i^{-1}_{G,H}(e_z) = e_x \otimes e_y$.

Wir repräsentieren $Z(G)$ in der Form $Z(G/H) \otimes Z(H)$ mit Hilfe zweier Codierungsabbildungen $\iota : G/H \to \{0,1\}^m$ und $\kappa : H \to \{0,1\}^k$ durch die Korrespondenzen

$$\begin{aligned} f = \sum_{g \in G} f(g) e_g \ &\leftrightarrow \sum_{x \in G/H,\, y \in H} f(r_{G,H}(x)y)\, e_x \otimes e_y \\ &\leftrightarrow \sum_{x \in G/H,\, y \in H} f(r_{G,H}(x)y)\, |\iota(x)\rangle \otimes |\kappa(y)\rangle. \end{aligned}$$

Es seien noch zwei Bemerkungen angefügt. Auf $Z(G/H) \otimes Z(H)$ können wir eine symmetrische Bilinearform durch

$$\langle f_{G/H} \otimes f_H, h_{G/H} \otimes h_H \rangle_{G,H} = \langle f_{G/H}, h_{G/H} \rangle_{G/H} \cdot \langle f_H, h_H \rangle_H$$

für $f_{G/H}, h_{G/H} \in G/H$ und $f_H, h_H \in H$ definieren. Man kann direkt nachrechnen, daß

$$\langle f, h \rangle_{G,H} = \langle i_{G,H}(f), i_{G/H}(h) \rangle_G$$

für alle $f, h \in Z(G/H) \otimes Z(H)$ gilt.

Seien $\chi \in \widehat{G/H}$ und $\psi \in \hat{H}$. Im allgemeinen ist $i_{G,H}(\chi \otimes \psi) \notin \hat{G}$. Dies gilt jedoch, wenn $r_{G,H}$ ein Homomorphismus ist. Diese Bedingung impliziert, daß es ein H' mit $G = H' \times H$ und $H' \cong G/H$ gibt.

Produktdarstellung der Fouriertransformation

Wie eben sei $H \subseteq G$ eine Untergruppe von G, $r_{G,H} : G/H \to G$ eine Repräsentantenfunktion und $i_{G,H} : Z(G/H) \otimes Z(H) \to Z(G)$.

Wir übertragen diese Situation auf $\hat{G}$. Nach Satz 1, (*iii*) können wir $(\widehat{G/H})$ als Untergruppe auffassen und $\hat{H}$ als Faktorgruppe $\hat{G}/(\widehat{G/H})$. Sei damit $\hat{r}_{G,H} : \hat{H} \to \hat{G}$ eine Repräsentantenfunktion. Analog wie oben erhalten wir $\hat{i}_{G,H} : Z(\hat{H}) \otimes Z((\widehat{G/H})) \to Z(\hat{G})$. Dann gilt

$$\begin{aligned}
F_G(e_g) &= (\#G)^{-1/2} \sum_{\chi \in \hat{G}} \chi(g^{-1}) e_\chi \\
&=_{\hat{i}_{G,H}} (\#G)^{-1/2} \sum_{\phi \in \hat{H},\, \psi \in (\widehat{G/H})} (\hat{r}_{G,H}(\phi)\psi)(g^{-1}) e_\phi \otimes e_\psi \\
&= \left((\#H)^{-1/2} \sum_{\phi \in \hat{H}} \hat{r}_{G,H}(\phi)(g^{-1}) e_\phi \right) \otimes \\
&\qquad\qquad \left((\#(G/H))^{-1/2} \sum_{\psi \in (\widehat{G/H})} \psi(g^{-1}H) e_\psi \right) \\
&= \left((\#H)^{-1/2} \sum_{\phi \in \hat{H}} \hat{r}_{G,H}(\phi)(g^{-1}) e_\phi \right) \otimes F_{G/H}(e_{gH}).
\end{aligned}$$

Dies wird als Produktdarstellung der Fouriertransformation bezeichnet. Gilt $G = H' \times H$ und sind $r_{G,H}$, $\hat{r}_{G,H}$ die entsprechenden Einbettungshomomorphismen, so gilt aus Symmetriegründen sogar

$$F_G(e_g) = F_{G/H'}(e_{gH'}) \otimes F_{G/H}(e_{gH}).$$

Die Produktdarstellung ist deshalb interessant für Quantencomputer, da zur Berechnung von F_G anstelle von $\#G$ Berechnungen von Charakterwerten nur $\#H + \#(G/H)$ solche Berechnungen erforderlich sind, den Rest übernimmt der Quantenparallelismus in Form des Tensorprodukts.

Die Prozedur kann auf die rechte Seite $F_{G/H}$ rekursiv angewendet werden, wenn G eine Kette von Untergruppen hat. Wir betrachten dazu $\{1\} = H_0 \subseteq \cdots \subseteq H_n = G$. Im i-ten Schritt entspricht G die Gruppe G/H_{i-1} und H die Gruppe H_i/H_{i-1}. Wir schreiben $\hat{r}_i = \hat{r}_{G/H_{i-1}, H_i/H_{i-1}} : (\widehat{H_i/H_{i-1}}) \to (\widehat{G/H_{i-1}})$. Damit ergibt sich

$$F_G(e_g) = (\#G)^{-1/2} \bigotimes_{i=1}^{n} \sum_{\phi_i \in \widehat{H_i/H_{i-1}}} \hat{r}_i(\phi_i)(g^{-1}H_{i-1}) e_{\phi_i}.$$

Hierin kann man noch g bei Bedarf sukzessive in Nebenklassenrepräsentanten bezüglich der H_i faktorisieren, sollte dies die Auswertung erleichtern.

Als Hauptbeispiel betrachten wir $G = \mathbb{Z}/2^n\mathbb{Z}$. Dann sind die Charaktere durch $\chi_j(k) = \exp(-2\pi ijk/2^n)$ für $0 \leq j \leq 2^n - 1$ gegeben. Weiter ist $H_i = \langle 2^{n-i} \rangle$ für $0 \leq i \leq n$, und die Gruppen H_i/H_{i-1} und $(\widehat{H_i/H_{i-1}})$ sind alle isomorph zu $\mathbb{Z}/2\mathbb{Z}$. Für die Repräsentantenabbildungen ergibt sich mit zusätzlichem Liften nach G: $r_j(0) = 1$, $r_j(1) = \tilde{\chi}_j$ mit $\tilde{\chi}_j(k) = \exp(2\pi ik/2^{n-j+1})$. Damit folgt bereits

$$\begin{aligned} F_G(|k\rangle) &= 2^{-n/2} \bigotimes_{\nu=1}^{n} \sum_{j\in\{0,1\}} \exp(2\pi ijk/2^{n-\nu+1})\, |j\rangle \\ &= 2^{-n/2} \bigotimes_{\nu=1}^{n} \sum_{j\in\{0,1\}} \exp(2\pi ijk/2^{\nu})\, |j\rangle, \end{aligned}$$

wobei k jeweils modulo $2^{n-\nu+1}$ bzw. 2^ν genommen werden kann. Wir wenden noch die erwähnte Faktorisierung von g und hier speziell k in Nebenklassenrepräsentanten an. In unserer Situation ergibt sich mit $k = \sum_{i=1}^{n} k_i 2^{i-1}$, $k_i \in \{0,1\}$ und $|k\rangle = |k_n \cdots k_1\rangle$ das folgende,

$$F_G(|k_n \ldots k_1\rangle) = 2^{-n/2} \bigotimes_{\nu=1}^{n} \left(|0\rangle + \Big(\prod_{j=1}^{\nu} \exp(2\pi i k_j 2^{j-\nu-1}) \Big) |1\rangle \right).$$

Damit berechnet sich jedes Qubit der Ausgabe als Hadamardtransformation $|k_\nu\rangle \mapsto 2^{-1/2}(|0\rangle + \exp(2\pi ik_\nu/2)|1\rangle)$, gefolgt von durch k_j mit $j < \nu$ kontrollierten Anwendungen der unitären Transformationen

$$R_{j,\nu} = \begin{pmatrix} 1 & 0 \\ 0 & \exp(2\pi i 2^{j-\nu-1}) \end{pmatrix}.$$

Eine Superposition der Eingabezustände $|k\rangle$ wird automatisch linear durch den entsprechenden Quantenschaltkeis zur Berechnung der Fouriertransformation abgebildet. Im vorliegenden Fall werden also $O(n^2)$ Gatter benötigt. Im klassischen Fall sind $O(2^{2n})$ trivialerweise und $O(n2^n)$ mit der schnellen Fouriertransformation erforderlich. Wie bereits erwähnt, kann mit dem Quantenschaltkreis in dieser Zeit $O(n^2)$ aber keine Fouriertransformation im klassichen Sinn ausgerechnet werden (d.h. als konrete Linearkombination und nicht als unbekannte Superposition).

Als weiteres Beispiel bemerken wir, das die n-fache Hadamardtransformation $H^{\otimes n}$ die Fouriertransformation auf der Gruppe $G = (\mathbb{Z}/2\mathbb{Z})^n$ darstellt.

Schnelle Fouriertransformation

Ergänzend soll kurz auf die klassische, schnelle Fouriertransformation eingegangen werden. Mit der Notation von oben und mit den Gleichungen $\hat{r}_{G,H}(\phi)\psi = \chi$, $r_{G,H}(x)y = g$ und $\psi(y) = 1$ schreiben wir

$$\begin{aligned} M_G &= (\#G)^{-1/2}\Big(\chi(g^{-1})\Big)_{\chi,g} \\ &= (\#G)^{-1/2}\Big(\hat{r}_{G,H}(\phi)(r_{G,H}(x)^{-1})\hat{r}_{G,H}(\phi)(y^{-1})\psi(r_{G,H}(x)^{-1})\psi(y^{-1})\Big) \\ &= (\#G)^{-1/2}\Big(\psi(r_{G,H}(x)^{-1})\hat{r}_{G,H}(\phi)(r_{G,H}(x)^{-1})\hat{r}_{G,H}(\phi)(y^{-1})\Big). \end{aligned}$$

Die Matrix M_G läßt sich daher in $\#H \times \#H$ Kästchen unterteilen, deren Zeilen mit $\phi \in \hat{H}$ und Spalten mit $y \in H$ indiziert werden. Jedes dieser Kästchen wiederum läßt sich in M_G durch $\psi \in (\widehat{G/H})$ zeilenweise und $x \in G/H$ spaltenweise indizieren. Die Kästchen haben die Form

$$\psi(r_{G,H}(x)^{-1})\Big(\hat{r}_{G,H}(\phi')(r_{G,H}(x)^{-1})\delta_{\phi',\phi}\Big)_{\phi',\phi}\Big(\hat{r}_{G,H}(\phi)(y^{-1})\Big)_{\phi,y},$$

wobei $\phi' \in \hat{H}$.

Die Berechnung der Fouriertransformation erfordert die Multiplikation von M_G mit einem Vektor von rechts. Ist das Produkt der ersten $\#H$ Zeilen von M_G für $\phi \in \hat{H}$ und $\psi = 1$ mit dem Vektor bekannt, so kann man leicht das Produkt für alle nachfolgenden Zeilen von M_G bestimmen, wegen der redundanten Form von M_G. Man muß nur die ersten $\#H$ Einträge des berechneten Vektors geeignet skalieren und anhängen. Da

$$\Big(\hat{r}_{G,H}(\phi)(y^{-1})\Big)_{\phi,y} = M_H,$$

läßt sich dieser Trick rekursiv anwenden.

Betrachten wir wieder $G = \mathbb{Z}/2^n\mathbb{Z}$ wie oben, so ergibt sich für die Anzahl der Rechenschritte $T_n = 2T_{n-1} + c2^n$ mit einer (von n unabhängigen, kleinen) Konstanten c. Es gilt $T_0 = 1$. Dann folgt $T_n = O(n2^n)$.

Hiervon gibt es viele Anwendungen. Eine besteht zum Beispiel darin, Konvolutionsprodukte mit n Termen in Zeit $O(\log(n)n)$ statt $O(n^2)$ zu berechnen. Hierzu zählt insbesondere die Polynom- und auch Integermultiplikation. Auf $Z(G)$ kann man eine Konvolutionsmultiplikation durch

$$(fh)(g) = \sum_{g=xy} f(x)h(y) = \sum_x f(x)h(gx^{-1})$$

definieren ($n = \#G$). Damit wird $Z(G)$ zum Gruppenring $\mathbb{C}[G]$ von G. Es ist dann nicht schwer zu zeigen, daß

$$F_G(fh)(\chi) = F_G(f)(\chi)F_G(h)(\chi)$$

für alle $\chi \in \hat{G}$ gilt. Damit verlagert man die Berechnung von fh auf die Berechnung von F_G (zweimal hin, einmal zurück) und die Berechung von $F_G(f)(\chi)F_G(h)(\chi)$ für alle χ, welches lineare Laufzeit $\#G$ erfordert.

Die dahinterstehende Logik ist, daß sich $\mathbb{C}[G]$ mit Hilfe orthogonaler Idempotenten als direktes Produkt von Kopien von $\mathbb{C}$ schreiben läßt. Dieses Umschreiben wird gerade durch die Fouriertransformation geleistet. Insofern handelt es sich bei der Fouriertransformation im Endeffekt um eine schnelle Berechnung des chinesischen Restsatzes. Man kann zum Beispiel Polynome $f, h \in \mathbb{C}[t]$ multiplizieren, in dem man sie in $R = \mathbb{C}[t]/\prod_{i=1}^{m}(t - a_i)$ mit $a_i \neq a_j$ und m groß genug multipliziert. Per chinesischem Restsatz ist $R \cong \prod_{i=1}^{m} \mathbb{C}[t]/(t - a_i) \cong \mathbb{C}^m$ Produkt von Kopien von $\mathbb{C}$. Das bedeutet, daß wir fh auch durch die Berechnung von $f(a_i)h(a_i)$ für alle i und Rekonstruktion nach $\mathbb{C}[t]$ ausrechnen können. Im Fall der Fouriertransformation betrachten wir implizit $R = \mathbb{C}[t]/(t^m - 1)$ und $a_j = \exp(2\pi ij/m)$. Für geeignete Werte von m, zum Beispiel $m = 2^n$, läßt sich dann effizient zwischen Polynomen f und Vektoren $(f(a_1), \ldots, f(a_m))$ mit der Fouriertransformation hin- und herschalten.