



## QUANTENTECHNOLOGIEN

# Licht trifft Knoten und Kanten

Sogenannte Graph-Zustände bieten Vorteile für quantentechnologische Anwendungen.

Daniel Bhatti und Stefanie Barz

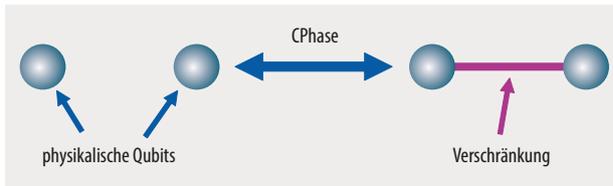
Dieser Artikel stellt Quantenanwendungen vor, die auf verschränkten Zuständen mit mehr als zwei Teilchen basieren. Dabei liegt der Fokus auf Graph-Zuständen. Diese lassen sich in allen physikalischen Systemen herstellen, in denen man einzelne Qubits manipulieren und verschränken kann. Beispiele sind Photonen, Atome, Ionen oder supraleitende Qubits. Wir konzentrieren uns auf photonische Systeme, da photonische Graph-Zustände Quantenkommunikation über weite Strecken, Quanteninternet oder -computing realisieren können.

Verschränkung spielt eine zentrale Rolle in den Quantentechnologien: In der Quantenkommunikation erlaubt sie es, geheime Schlüssel auszutauschen, im Quantencomputing sind verschränkende Gatteroperationen essenziell. Besonders deutlich zeigen sich die speziellen Eigenschaften der Quantenmechanik an verschränkten Zuständen mit zwei Teilchen [1]. Eine Messung an einem Teilchen kann den Zustand des Partnerteilchens instantan und unabhängig von der Entfernung verändern.

Aber auch die Verschränkung von mehr als zwei Teilchen wird durch die sich stetig entwickelnden Quantentechnologien immer wichtiger. Besonders die Herstellung sogenannter Graph-Zustände beschäftigt aktuell viele experimentelle Forschungsgruppen. Ein Graph-Zustand ist definiert durch einen mathematischen Graphen. Ein solcher besitzt Knoten und Kanten, welche die Quantenbits sowie deren Verschränkung darstellen. Das Quantenbit (kurz Qubit) ist die fundamentale Einheit der Quanteninformationsverarbeitung. Ein allgemeiner Ein-Qubit-Zustand lässt sich schreiben als  $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$  mit den Basiszuständen  $|0\rangle$  und  $|1\rangle$  [2]. Die Koeffizienten  $\alpha$  und  $\beta$  sind komplexe Zahlen, für die gilt  $|\alpha|^2 + |\beta|^2 = 1$ .

Betrachten wir einen einfachen Graphen mit zwei Knoten, stellt jeder Knoten ein Qubit dar (Abb. 1, links) [3]. Diese werden zunächst jeweils in einem Superpositionszustand  $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$  präpariert. Der Gesamtzustand des Systems ist damit:

$$|+\rangle|+\rangle = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle + |11\rangle). \quad (1)$$



**Abb. 1** Zunächst befinden sich die beiden Qubits unabhängig voneinander jeweils im Anfangszustand  $|+\rangle$ : Sie sind als unverbundene Knoten gezeigt (links). Die Anwendung eines CPhase-Gatters entlang einer Kante erzeugt Verschränkung zwischen ihnen (rechts).

Die Knoten eines Graphen können durch Kanten verbunden sein (**Abb. 1**, rechts). Um einen solchen Zustand physikalisch aus einzelnen Qubits herzustellen, werden entlang der Kanten verschränkende Gatter angewendet, konkret CPhase-Gatter. Deren Funktionsweise ist durch die folgende Übergangstabelle gegeben:

$$\begin{array}{ll} |00\rangle \rightarrow +|00\rangle & |01\rangle \rightarrow +|01\rangle \\ |10\rangle \rightarrow +|10\rangle & |11\rangle \rightarrow -|11\rangle. \end{array}$$

Demnach erfährt ausschließlich der Term  $|11\rangle$  eine Phasenänderung von  $-1$ . Durch Anwenden des CPhase-Gatters auf den Zustand in Gleichung (1) erhalten wir:

$$\text{CPhase } |+\rangle|+\rangle = \frac{1}{2} (|00\rangle + |01\rangle + |10\rangle - |11\rangle). \quad (2)$$

Dies ist ein verschränkter Zustand, also ein Graph-Zustand mit zwei Qubits! Obwohl sich dieser von Gleichung (1) scheinbar nur durch ein Vorzeichen unterscheidet, wirkt sich die Messung des einen Qubits nun direkt auf den Zustand des anderen Qubits aus. Die beiden Qubits sind somit maximal quantenmechanisch verschränkt.

### Lego mit Graph-Zuständen

CPhase-Gatter eignen sich, um größere Graph-Zustände zu erzeugen. Dabei können wir einzelne Bausteine wie Legosteine zu verschränkten Zuständen mit mehreren Qubits

zusammensetzen (**Abb. 2**). Ausgehend von verschiedenen mathematischen Graphen lässt sich der zugehörige Graph-Zustand nach der gleichen Grundregel erzeugen: Jedes einzelne Qubit im Anfangszustand  $|+\rangle$  präparieren und anschließend CPhase-Gatter auf die Paare von Qubits anwenden, die durch eine Kante verbunden sind. Der Graph gibt die Struktur der Verschränkung vor, aus der sich mögliche Anwendungen in den Quantentechnologien ergeben.

Besonders wichtig sind zwei Arten von Graph-Zuständen:

- Vollständig verbundene Graphen, bei denen jeder Knoten mit allen anderen Knoten verbunden ist: Diese Graphen sind Greenberger-Horne-Zeilinger-Zustände (GHZ), wobei der kleinste GHZ-Zustand aus drei Qubits besteht und folgendermaßen dargestellt werden kann:

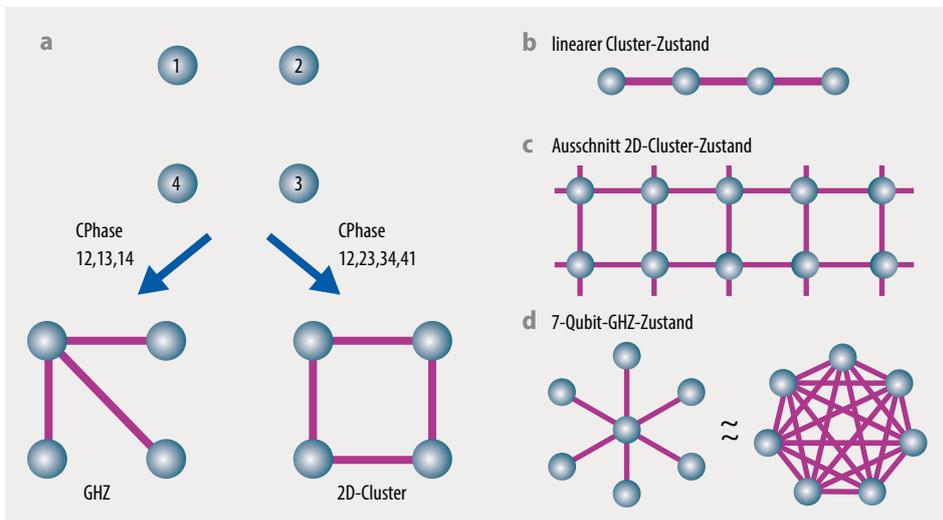
$$|\text{GHZ}\rangle = \frac{1}{\sqrt{2}} (|000\rangle + |111\rangle). \quad (3)$$

GHZ-Zustände sind historisch relevant für fundamentale Fragestellungen der Quantenmechanik [4] und finden besonders in der Quantenkommunikation Anwendung.

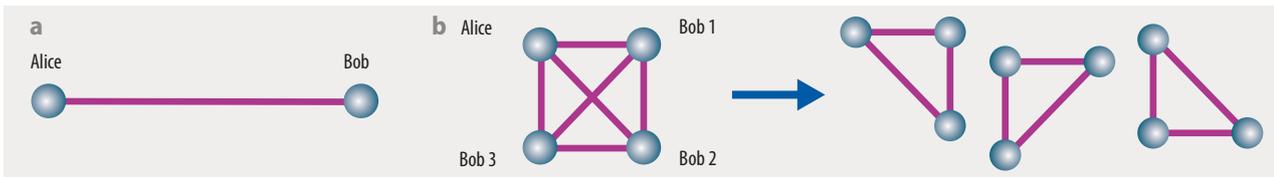
- Graph-Zustände, die durch ein zweidimensionales Gitter dargestellt werden: Diese sog. Cluster-Zustände sind wichtig für das Quantencomputing.

Experimentell herstellen lassen sich Graph-Zustände beispielsweise in photonischen Systemen (**Infokasten** Photonische Graph-Zustände) [5, 6, 7]. Die Basiszustände  $|0\rangle$  und  $|1\rangle$  sind dabei in verschiedenen Freiheitsgraden kodiert, beispielsweise mittels Polarisation oder verschiedener räumlicher Pfade. Die Wahrscheinlichkeitsamplitude für eine Polarisation bzw. einen Pfad entspricht den Koeffizienten  $\alpha$  und  $\beta$  oben.

Die Erzeugung photonischer Graph-Zustände basiert oftmals auf verschränkten Photonenpaaren. Optische Elemente, wie CPhase-Gatter oder allgemeinere Fusionsgatter, fügen diese zu größeren Graph-Zuständen zusammen (**Infokasten**). Diese photonischen Gatter funktionieren meist probabilistisch, d. h. eine Gatteroperation ist nicht in jedem Fall erfolgreich. Mit diesen Methoden gelang es, GHZ-Zustände mit bis zu zehn Photonen zu realisieren, unter Ausnutzung mehrerer Freiheitsgrade sogar 18 Qubits [8].



**Abb. 2** Ausgehend von vier unabhängigen Qubits (a) lassen sich verschiedene Graph-Zustände realisieren, indem CPhase-Gatter entlang der Kanten angewendet werden. Gezeigt sind ein GHZ-Zustand und ein 2D-Cluster-Zustand mit je vier Qubits. Beispiele für Graph-Zustände sind in (b) bis (d) zu sehen. Die zugehörigen Zustände der Repräsentationen von GHZ-Zuständen (d) sind bis auf bestimmte lokale (unitäre) Transformationen gleich.



**Abb. 3** Alice und Bob teilen sich einen verschränkten Zustand (a), um einen Quantenschlüssel auszutauschen. Für das Conference Key Agreement teilen sich Alice und drei Bobs einen verschränkten 4-Teilchen-GHZ-Zustand (b). Im anonymen Fall lassen sich Knoten des Graph-Zustands und damit Parteien anonym entfernen, sodass der Schlüsselaustausch zwischen den restlichen Parteien mithilfe eines kleineren GHZ-Zustandes stattfindet.

### Quantenkommunikation mit Netzen

Ein verschränkter Zustand aus zwei Qubits kann zur Quantenkommunikation zwischen zwei Parteien dienen. Verfügenden Sender (Alice) und Empfänger (Bob) jeweils über ein Qubit eines verschränkten Zustands (**Abb. 3a**), können sie Messungen an diesem durchführen. Deren Ergebnisse sind korreliert und erlauben es zusammen mit dem Abgleich der Messbasen, einen Schlüssel auszutauschen, um einen möglichen Lauscher aufzuspüren (Quantenschlüsselaustausch, Quantum Key Distribution) [9].

Graph-Zustände mit mehreren Qubits ermöglichen komplexere Anwendungen der Quantenkommunikation mit mehreren Sendern bzw. Empfängern. Hier sind insbesondere photonische Graph-Zustände relevant, da sich diese über optische Netzwerke verteilen lassen.

Ein Beispiel ist der Schlüsselaustausch in einem Quantennetzwerk mit mehr als zwei Parteien (Conference

Key Agreement) [10]. Hier ist es möglich, einen Quantenschlüsselaustausch jeweils paarweise zwischen zwei Parteien zu realisieren und mittels klassischer Kommunikation einen Schlüssel über das gesamte Netzwerk zu generieren.

Eine Alternative für den Schlüsselaustausch stellen GHZ-Zustände dar. Die Nutzer in einem Netzwerk teilen sich hierfür zunächst einen GHZ-Zustand:  $|\text{GHZ}\rangle = \frac{1}{\sqrt{2}}(|00\dots 0\rangle + |11\dots 1\rangle)$ , sodass jeder Nutzer ein Qubit des Zustands erhält, beispielsweise ein Photon (**Abb. 3b**). Analog zum Protokoll mit zwei Parteien finden Messungen an dem Zustand statt. Wählen alle die Messbasis ( $|0\rangle/|1\rangle$ ), so sorgt der GHZ-Zustand dafür, dass alle entweder ein Bit „0“ oder „1“ erhalten. Diese Runden erzeugen den Schlüssel. Um einen Lauscher im System zu entdecken, finden zwischen durch zufällig Runden in anderen Messbasen statt. Das Vorhandensein eines Lauschers verändert das Ergebnis dieser „Testrunden“. Deshalb erlaubt es der klassische Austausch

## Photonische Graph-Zustände

### Erzeugung verschränkter Photonen

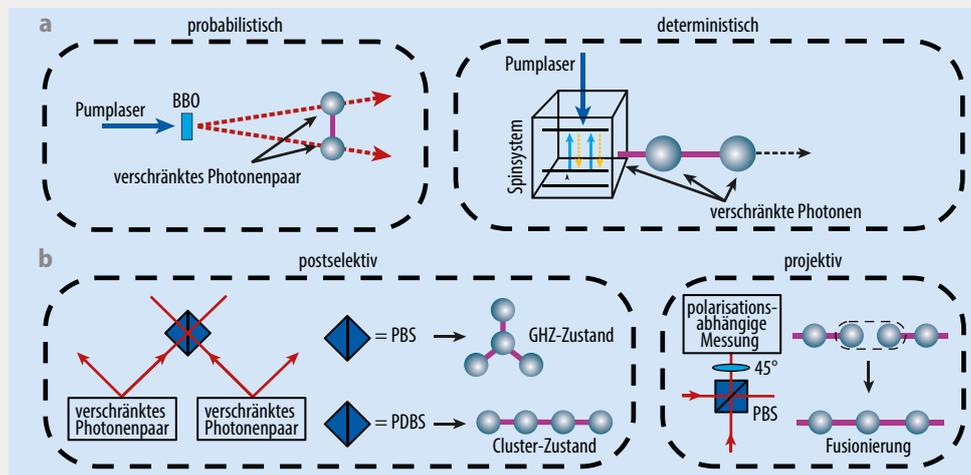
- Verschränkte Photonenpaare lassen sich probabilistisch unter Ausnutzung von Prozessen wie spontaner parametrischer Fluoreszenz erzeugen (**Abb. a**). Dazu wird ein nichtlinearer Kristall (z. B. BBO) mit Laserlicht gepumpt, sodass aus einzelnen Pump-Photonen zwei Tochter-Photonen mit der halben Energie entstehen. Spezielle geometrische Anordnungen sorgen dafür, dass deren Polarisationsfreiheitsgrade verschränkt sind.
- Mithilfe eines Spinsystems sind Cluster-Zustände deterministisch erzeugbar. Dies wurde für Zustände aus bis zu fünf Qubits demonstriert.

### Photonische Fusionsgatter

Allgemein lassen sich Fusionsgatter basierend auf linearer Optik wie polarisierenden Strahlteilern (PBS) und Wellenplatten erzeugen. Diese sind probabilistisch, also nur in einem bestimmten Prozentsatz der Fälle erfolgreich.

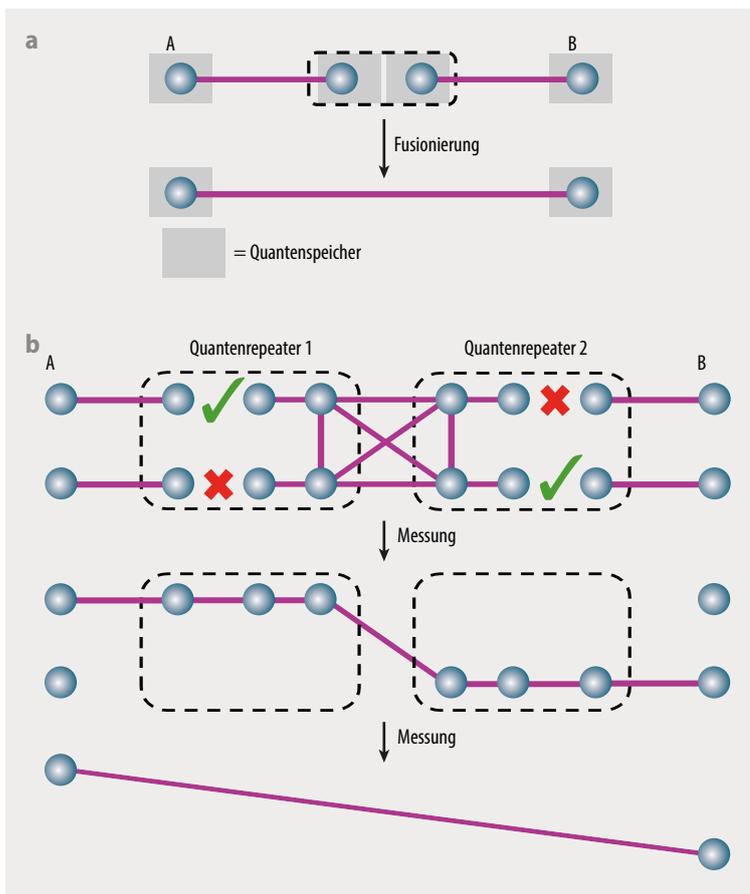
- Zwei verschränkte Photonenpaare lassen sich mithilfe eines PBS zu einem GHZ-Zustand mit vier Qubits fusionieren (**Abb. b**): Startet man mit jeweils zwei Paaren im Zustand  $\frac{1}{\sqrt{2}}(|\text{HV}\rangle - |\text{VH}\rangle) \otimes \frac{1}{\sqrt{2}}(|\text{HV}\rangle - |\text{VH}\rangle)$ , wobei H bzw. V ein horizontal bzw. vertikal polarisiertes Photon beschreiben, und sendet jeweils eines der Photonen durch einen PBS, so folgt:  $\frac{1}{\sqrt{2}}(|\text{HVVH}\rangle + |\text{VHHV}\rangle)$ . Dabei werden nur Fälle mit jeweils einem einzelnen Photon an jedem Ausgang des Strahlteilers berücksichtigt (Postselektion). Die Fusionsoperation ist daher probabilistisch. Hier kodiert  $|\text{H/V}\rangle$  den Zustand  $|0/1\rangle$ .

- Mithilfe polarisationsabhängiger Strahlteiler (PDBS) ist ein einfaches probabilistisches CPhase-Gatter realisierbar. Damit lassen sich zwei unabhängige Photonen miteinander verschränken oder zwei verschränkte Photonenpaare zu einem Cluster-Zustand zusammenfügen. PDBS transmittieren horizontal polarisiertes Licht mit 100 Prozent und haben ein Teilungsverhältnis von (30/70) Prozent für vertikal polarisiertes Licht (Transmission/Reflexion). Das Gatter beruht darauf, dass nur für zwei vertikal polarisierte Photonen ein Phasensprung von  $\pi$  auftritt. Für die Fälle mit genau einem Photon an jedem Ausgang entspricht dies einem CPhase-Gatter.
- Allgemeine Fusionsgatter können mithilfe eines PBS und einer Wellenplatte zwei Cluster-Zustände fusionieren. Hierbei wird eines der Photonen in einer bestimmten Polarisationsbasis gemessen, ein bestimmtes Resultat zeigt die Fusionierung der restlichen Photonen an.



nach Science 354, 416 (2016)

nach PRL 95, 010501 (2005)



**Abb. 4** Der Quantenrepeater in (a) beruht auf einer Verbindung von zwei Links durch eine bestimmte Art der Fusionierung. Alternativ lässt sich ein Quantenrepeater mittels Graph-Zuständen erzeugen (b).

der Messbasen und der Messergebnisse zu überprüfen, ob der Schlüsselaustausch funktioniert hat oder von einem Lauscher unterbrochen wurde.

Das Conference Key Agreement mit GHZ-Zuständen ermöglicht zusätzlich Anonymität im Netzwerk: Die Idee ist dabei, nur in einem Teil des Netzwerks einen Schlüssel auszutauschen, während die Identität der beteiligten Parteien verborgen bleibt. Hierfür nutzt man die Eigenschaften des GHZ-Zustands. Wählen die unbeteiligten Parteien entsprechende Messbasen für ihre Messungen, werden ihre Knoten aus dem Graphen gelöscht. Übrig bleibt ein kleinerer GHZ-Zustand, den sich nur noch die beteiligten Parteien teilen (**Abb. 3b**). Dadurch erfährt keine der Parteien, wer an der Kommunikation beteiligt ist und wer nicht [11]. Das Conference Key Agreement, sowohl in der ursprünglichen als auch der anonymen Form, gelang bereits in einem photonischen Netzwerk mit vier Parteien [12, 13].

Ein weiteres Beispiel ist das Quantum Secret Sharing. Dabei wird eine Information so aufgeteilt, dass jeder Teil für sich alleine keine Hinweise auf die geheime Information gibt [14]. Dies geschieht mittels GHZ- oder allgemeineren Graph-Zuständen [15]. Die Parteien teilen sich einen Zustand und führen auf dem jeweiligen Qubit eine Messung in einer bestimmten Basis durch. Alle Messergebnisse zusammen ermöglichen es, den Schlüssel zu rekonstruieren. Jedes Messergebnis für sich enthält keine Information über den Ursprungszustand.

## Verluste vermeiden

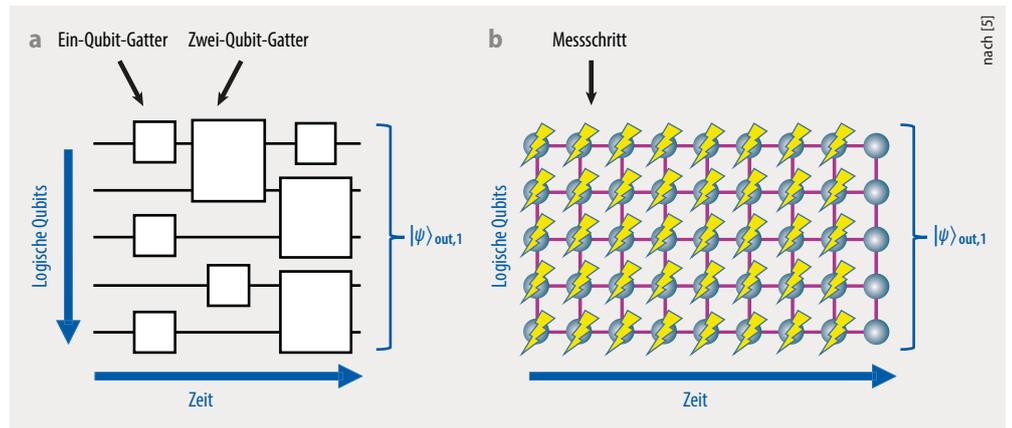
In Quantenkommunikations-Technologien limitieren optische Verluste die Übertragungsraten bzw. die Distanzen, über die Quantenkommunikation möglich ist, besonders in Systemen mit optischen Glasfasern. Quantenrepeater helfen, dies zu umgehen [16]. Solche Zwischenstationen speichern die photonischen Zustände (**Abb. 4a**) und beruhen meist auf atomaren oder Festkörper-basierten Systemen. Dank der Speicherung lässt sich eine große Distanz in mehrere kürzere Links aufteilen, die unabhängig voneinander aufzubauen sind. Dies ermöglicht eine längere Gesamtdistanz als die direkte Übertragung. Zu den Anforderungen an solche Systeme gehören z. B. die effiziente Wechselwirkung des Speichersystems mit dem photonischen System, eine lange Speicherzeit oder eine hohe Güte des gespeicherten Zustands. Diese gleichzeitig zu erfüllen, ist herausfordernd.

Alternativ können komplexere Graph-Zustände zum Einsatz kommen: In einem optischen Quantenrepeater erzeugen Zwischenstationen komplexe Graph-Zustände, an denen einzelne Qubits wie Blätter an einem Baum hängen (**Abb. 4b**) [17]. Diese werden zur nächsten Repeaterstation geschickt und fusionieren dort mit den Blätter-Qubits der nächsten Station, um einen größeren Zustand und somit längeren Link aufzubauen. Die Fusionierung ist probabilistisch, wobei mehr parallele Fusionierungsversuche die Erfolgswahrscheinlichkeit erhöhen. Sobald eine Fusionierung pro Quantenrepeater, also an jeder Seite des Graph-Zustands, erfolgt ist, lassen sich die übrigen und nicht mehr benötigten Knoten durch Messungen der entsprechenden Qubits aus dem Netzwerk entfernen. Das Fortführen dieses Schemas über mehrere optische Repeaterstationen verbindet die gewünschten Sender und Empfänger.

## Graph-Zustände im Quantencomputing

Im gatterbasierten Quantencomputing werden Quantengatter auf Eingangszustände angewendet, um Quantenrechnungen auszuführen (**Abb. 5a**) [18, 19]. Den Ausgangspunkt eines messbasierten One-Way-Quantencomputers stellt hingegen ein Cluster-Zustand dar (**Abb. 5b**). Dessen Zeilen entsprechen den logischen Qubits, d. h. der Anzahl an Qubits, mit der effektiv gerechnet wird. Der Algorithmus ergibt sich als Sequenz von Ein-Qubit-Messungen. Im ersten Schritt werden die Qubits in der ersten Spalte in einer bestimmten Basis gemessen. Da diese mit dem restlichen Zustand verschränkt sind, ändert sich, je nach Messbasis und -ergebnis, der verbleibende Zustand. Dann folgt die zweite Spalte, wieder in einer bestimmten Basis. Diese Spalte hängt vom Ergebnis der ersten Messung ab. Wieder ändert sich der verbleibende Cluster-Zustand, da dieser auch mit den Qubits in der zweiten Spalte verschränkt war. Sobald nur noch eine letzte Spalte des Cluster-Zustands übrig bleibt, ist der Ausgangszustand erreicht. Diese sequenziellen Messungen am Cluster-Zustand können Quantengatter implementieren. Die Wahl der Messbasen bestimmt das Gatter oder den Algorithmus (**Infokasten MBQC**).

**Abb. 5** Im gatterbasierten Quantencomputing setzt sich ein Quantenalgorithmus aus einer Serie von Ein- und Zwei-Qubit-Gattern zusammen (a). Das Ergebnis der Quantenrechnung wird nach Durchführung des Schaltkreises durch eine Messung aller Qubits bestimmt. Im messbasierten One-Way-Modell legt die Sequenz von Ein-Qubit-Messungen (Blitze) an einem Cluster-Zustand fest, welcher Quantenschaltkreis implementiert wird (b). Die horizontalen Linien stellen die logischen Qubits dar, die Spalten legen eine zeitliche Reihenfolge fest.



nach [5]

In photonischen Systemen ist die direkte Realisierung von Mehr-Qubit-Gattern schwierig, da Photonen nicht wechselwirken. Weil allerdings Graph-Zustände hergestellt werden können, eignet sich das messbasierte Modell nun besonders für die Realisierung des photonischen Quanten-Computings. Messbasiertes Quantencomputing gelang bereits mit vier photonischen Qubits [20, 21], wobei sich ein Satz an Ein-Qubit- und Zwei-Qubit-Gattern sowie Quantenalgorithmus implementieren ließen. Derzeit versuchen Forschende, effiziente Varianten dieser Methode zu entwickeln. Eine davon ist das fusionsbasierte Quantencomputing, das auf ähnlichen Grundkonzepten basiert und hilft, die eingesetzten Ressourcen zu optimieren.

Sehr wichtig im Quantencomputing ist die Fehlerkorrektur (Quantum Error Correction), die Quantenzu-

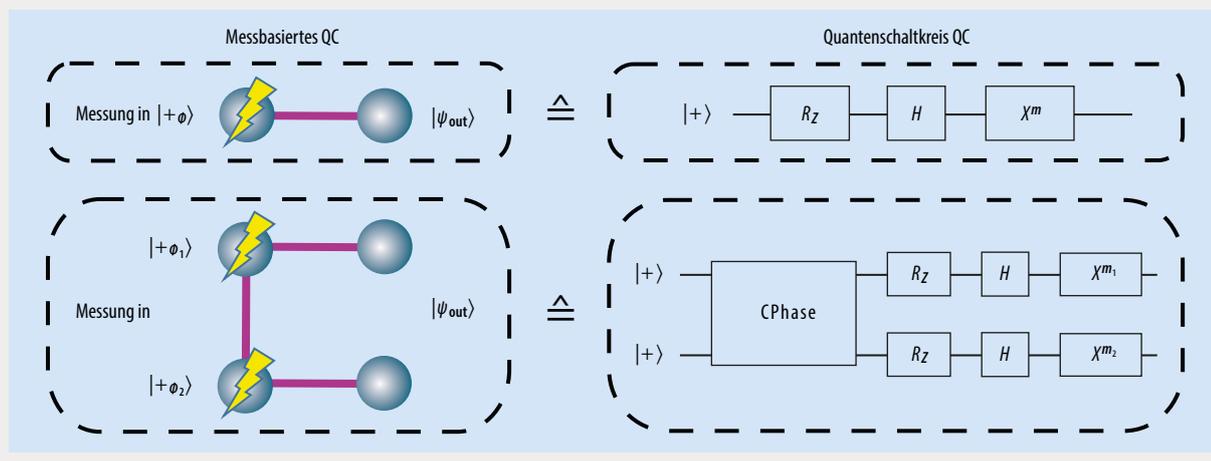
stände bzw. -information gegen auftretende Fehler schützen soll [22]. Eine Möglichkeit besteht darin, jedes logische Qubit in einen weiteren Graph-Zustand aus mehreren physikalischen Qubits zu kodieren [3]. Ein alternativer Ansatz im messbasierten Modell ist die Nutzung von 3D-Cluster-Zuständen, um topologische Codes zu realisieren [23]. In photonischen Systemen sind neben den Gatterfehlern vor allem Photonenverluste kritisch. Fehlerkorrigierende Codes müssen daher so angelegt sein, dass ein bestimmter Anteil an Photonenverlusten tolerierbar ist. Erste Schritte zur Fehlerkorrektur wurden in photonischen Systemen mit vier und fünf Qubits demonstriert [24, 25, 26]. Demnach lassen sich bestimmte Arten von Fehlern wie Phasen- oder Bitflipfehler sowie Verluste einzelner Photonen auf den logischen Qubits detektieren.

## Messbasiertes Quantencomputing (MBQC)

Das messbasierte Quantencomputing (MBQC) lässt sich an einem Cluster-Zustand mit zwei Qubits  $|\psi\rangle = 1/2(|00\rangle + |01\rangle + |10\rangle - |11\rangle)$  verdeutlichen. Misst man das erste Qubit in der Basis  $|+\phi\rangle = 1/\sqrt{2}(|0\rangle + e^{i\phi}|1\rangle)$ , ist der Ausgangszustand des zweiten Qubits gegeben durch  $|\psi_{out}\rangle = X^m H R_z(-\phi) |+\rangle$ . Der Ausgangszustand hängt also vom Messwinkel  $\phi$  sowie vom Messergebnis  $m$  ab. Die Operatoren  $H$  (Hadamard-Gatter) und  $R_z$  (z-Rotation) bezeichnen Ein-Qubit-Gatter, deren spezielle Form für dieses Beispiel nicht relevant ist. Der Operator  $X$  ist durch den entsprechenden Pauli-Operator gegeben und wird nur angewendet, wenn das Messergebnis  $m$  am ersten Qubit

das Resultat „1“ ergeben hat. Effektiv wurde also ein Ein-Qubit-Gatter durchgeführt. Bei weiteren Messungen wäre das Messergebnis  $m$  bei der Wahl der darauffolgenden Messbasis zu berücksichtigen. Daraus ergeben sich die notwendige Adaptivität und die zeitliche Abfolge der Messungen. Blitze stellen jeweils dar, welche Qubits gemessen werden.

Die vertikalen Linien im Cluster-Zustand sind nötig, um Zwei-Qubit-Gatter zu implementieren. Durch Messungen in der Basis  $|0\rangle / |1\rangle$  lassen sich Qubits aus dem Cluster-Zustand entfernen, um die Form des Graphen auf einen bestimmten Algorithmus anzupassen.



## Eine Wolke aus Quanten

Die Kombination von messbasiertem Quantencomputing mit Quantenkommunikation macht Quantum Cloud Computing in einem Netzwerk realisierbar (Blind Quantum Computing) [27]. Hierbei kann ein Nutzer eine Quantenrechnung an einen Server (Quantencomputer) delegieren, wobei sowohl die Daten als auch der Algorithmus selbst verschlüsselt bleiben. Diese blinde Rechnung kombiniert Sicherheit und schnellere Rechnungen. Das Quantum Computing in der Cloud läuft nach dem Prinzip des messbasierten Quantum Computings ab: Dazu generiert der Nutzer verschlüsselte Messinstruktionen, angepasst an den Zustand der generierten Qubits, und sendet diese zum Server. Der Server führt Messungen nach verschlüsselten Messinstruktionen auf einem ihm unbekanntem Zustand durch und erhält ein verschlüsseltes Ergebnis. Dieses schickt er an den Nutzer, dem alle Informationen vorliegen, um das Ergebnis zu entschlüsseln. Nach diesem Prinzip lassen sich allgemeine Quantenrechnungen an einen Server auslagern.

Blind Quantum Computing fand bereits in einem photonischen System mit vier Qubits statt. Hierbei zeigte sich modellhaft, dass Quanten-Gatter sowie ganze Quanten-Algorithmen sicher auf Quanten-Server auszulagern sind [28].

## Ausblick und Skalierung

Über die hier betrachteten Beispiele hinaus besitzen Graph-Zustände viele weitere Anwendungsmöglichkeiten, beispielsweise in der vernetzten Quantenmetrologie. Theoretisch wie technologisch ist die Erforschung effizienter Methoden zur Erzeugung photonischer Graph-Zustände ein sehr aktives Forschungsfeld.

Auf theoretischer Seite geht es unter anderem darum, neue, effiziente Konzepte zu entwickeln, um die Zustände zu erzeugen. Beispielsweise erhöhen zusätzliche Hilfsphotonen die Erfolgswahrscheinlichkeiten für Gatter. Ebenso wichtig ist es, neue Anwendungsmöglichkeiten zu erforschen sowie existierende Konzepte zu verbessern, um die benötigten Ressourcen zu minimieren. Vielversprechend bezüglich der Fehlertoleranz und Skalierbarkeit erscheint es, auch kontinuierliche Variablen auszunutzen.

Auf technologischer Seite ist es herausfordernd, verlustarme optische Systeme zu entwickeln. Hier spielt die integrierte Optik eine wichtige Rolle. Sie ermöglicht es, Zustände mittels miniaturisierter optischer Schaltkreise zu erzeugen, und trägt damit entscheidend zur Skalierbarkeit bei. Vollintegrierte Systeme mit Graph-Zuständen aus bis zu vier Qubits existieren bereits.

Ein weiterer Ansatz liegt in der deterministischen und direkten Erzeugung von Graph-Zuständen bzw. in der Realisierung deterministischer Gatteroperationen. Systeme, deren interne Freiheitsgrade sich mit photonischen Freiheitsgraden verschränken lassen, bieten die Möglichkeit, Graph-Zustände direkt zu erzeugen. Dies gelang mit einem Quantenpunktsystem [29]. Deterministische CPhase-Gatter sind mithilfe atomarer Systeme möglich. Hier sind

bestimmte Sequenzen an Laserpulsen und Operationen wie das CPhase-Gatter im Prinzip deterministisch realisierbar. Diese Ansätze sind Gegenstand aktueller Forschung und stellen wichtige technologische Herausforderungen dar.

## Literatur

- [1] J. L. Miller, *Physics Today* **69**, 14 (2016)
- [2] I. L. Chuang und M. A. Nielsen, *J. Mod. Opt.* **44**, 2455 (1997)
- [3] M. Hein et al., arXiv:quantph/0602096 (2006)
- [4] D. M. Greenberger et al., *Am. J. Phys.* **58**, 1131 (1990)
- [5] S. Barz, *J. Phys. B*, **48**, 083001 (2015)
- [6] F. Flamini, N. Spagnolo und F. Sciarrino, *Rep. Prog. Phys.* **82**, 016001 (2018)
- [7] S. Slussarenko und G. J. Prydey, *Appl. Phys. Rev.* **6**, 041303 (2019)
- [8] X. Wang et al., *Phys. Rev. Lett.* **120**, 260502 (2018)
- [9] A. K. Ekert, *Phys. Rev. Lett.* **67**, 661 (1991)
- [10] G. Murta et al., *Adv. Quantum Technol.* **3**, 2000025 (2020)
- [11] F. Hahn, J. de Jong und A. Pappa, *PRX Quantum* **1**, 020325 (2020)
- [12] M. Proietti et al., arXiv:2002.01491 (2020)
- [13] C. Thalacker et al., *New J. Phys.* **23**, 083026 (2021)
- [14] M. Hillery, V. Bužek und A. Berthiaume, *Phys. Rev. A* **59**, 1829 (1999)
- [15] B. A. Bell et al., *Nat. Commun.* **5**, 1 (2014)
- [16] W. J. Munro et al., *IEEE J. Sel. Top. Quantum Electron.* **21**, 78 (2015)
- [17] K. Azuma, K. Tamaki und H. Lo, *Nat. Commun.* **6**, 1 (2015)
- [18] R. Raussendorf und H. J. Briegel, *Phys. Rev. Lett.* **86**, 5188 (2001)
- [19] R. Raussendorf und H. J. Briegel, arXiv:quantph/0010033 (2001)
- [20] P. Walther et al., *Nature* **434**, 169 (2005)
- [21] R. Prevedel et al., *Nature* **445**, 65 (2007)
- [22] S. J. Devitt, W. J. Munro und K. Nemoto, *Rep. Prog. Phys.* **76**, 076001 (2013)
- [23] H. J. Briegel et al., *Nat. Phys.* **5**, 19 (2009)
- [24] S. Barz et al., *Phys. Rev. A* **90**, 042302 (2014)
- [25] B. A. Bell et al., *Nat. Commun.* **5**, 1 (2014)
- [26] C. Vigliar et al., *Nat. Phys.* **17**, 1137 (2021)
- [27] J. F. Fitzsimons, *npj Quantum Information* **3**, 1 (2017)
- [28] S. Barz et al., *Science* **335**, 303 (2012)
- [29] I. Schwartz et al., *Science* **354**, 434 (2016)

## Die Autor:innen



**Daniel Bhatti** promovierte an der Universität Erlangen-Nürnberg in theoretischer Quantenoptik. Derzeit ist er als Postdoc an der Universität Stuttgart tätig. Neben der Quantenoptik beschäftigt er sich mit Quantum Computing.

**Stefanie Barz** ist Professorin für Quanteninformation und -technologie an der Universität Stuttgart mit Schwerpunkt auf photonischen Quantensystemen. Zuvor war sie als Postdoc an der Universität Oxford tätig und hat an der Universität Wien in Physik promoviert.



**Dr. Daniel Bhatti** und **Prof. Dr. Stefanie Barz**, Quantum Information & Technology, Universität Stuttgart, Allmandring 3, 70569 Stuttgart