

NISQ, CZYLI DLACZEGO KOMPUTERY KWANTOWE ISTNIEJĄ I JEDNOCZEŚNIE NIE ISTNIEJĄ

Tomasz Lewandowski
Uniwersytet Mikołaja Kopernika w Toruniu
Wydział Matematyki i Informatyki
tomaszlew@mat.umk.pl

Abstract. *This paper presents an overview of Noisy Intermediate-Scale Quantum (NISQ) computing. It discusses key hardware platforms, error sources, and quantum error correction methods. Special attention is given to scalability limitations and their impact on practical applications. The paper also outlines implications for cryptography and quantum education.*

1. Wstęp

Żyjemy w czasach niewątpliwie ciekawych. Gdzieś pomiędzy odkryciem mechaniki kwantowej a zbudowaniem w pełni praktycznego komputera kwantowego. Mimo że znamy już bardzo dobrze matematyczne podstawy zjawisk kwantowych, to dopiero zaczynamy uczyć się, jak zamienić je w działające urządzenia obliczeniowe. Obecny etap rozwoju nazywany jest erą NISQ (Noisy Intermediate-Scale Quantum), czyli okresem, w którym dysponujemy już średniej skali procesorami kwantowymi, ale ich działanie wciąż jest silnie zakłócanie przez szumy i błędy [5].

Jak zauważa John Preskill w pracy dotyczącej komputerów NISQ [4], urządzenia kwantowe które znamy obecnie, znajdują się w fazie przejściowej. To znaczy że są wystarczająco duże, aby wykraczać poza możliwości klasycznej symulacji, ale jednocześnie zbyt małe, aby wykorzystywać swój pełen potencjał. To właśnie ten stan pomiędzy definiuje wyzwanie współczesnym inżynierom kwantowym.

W ostatnich latach coraz częściej pojawia się również pojęcie „Q-Day”, czyli hipotetycznego momentu, w którym komputery kwantowe osiągną na tyle dużą moc obliczeniową, że będą w stanie łamać powszechnie stosowane systemy kryptograficzne [22]. Choć nie jest to jeszcze rzeczywistość, sama możliwość takiego scenariusza znacząco wpływa na rozwój kryptografii postkwantowej oraz strategii bezpieczeństwa cyfrowego [19].

Celem niniejszej pracy jest przegląd najważniejszych aspektów technicznych komputerów kwantowych oraz analiza kluczowych problemów, z którymi mierzy się współczesna inżynieria kwantowa. Przedstawione są główne technologie sprzętowe, takie jak

kubity nadprzewodzące, pułapki jonowe, układy fotoniczne oraz systemy oparte na atomach neutralnych. Szczególna uwaga jest poświęcona problemom korekcji błędów, skalowalności oraz ograniczeniom fizycznym obecnych architektur.

2. Kubit jako podstawowa jednostka informacji kwantowej

Podstawową jednostką informacji w klasycznych komputerach jest bit. Bit może przyjmować jedną z dwóch wartości: 0 lub 1. Wszystkie współczesne systemy cyfrowe, od prostych kalkulatorów po superkomputery, operują właśnie na takich binarnych stanach [13].

Analogiczną rolę w komputerach kwantowych pełni kubit (ang. quantum bit) [13]. W przeciwieństwie do klasycznego bitu kubit nie jest ograniczony wyłącznie do stanów 0 lub 1. Znajduje się w tzw. superpozycji tych stanów [13]. Formalnie dwa podstawowe stany kubitów oznaczają się symbolami $|0\rangle$ oraz $|1\rangle$. Symbole te pochodzą z notacji Diraca powszechnie stosowanej w mechanice kwantowej [14], ale można je traktować jako kwantowe odpowiedniki klasycznych wartości 0 i 1.

3. Architektury sprzętowe komputerów kwantowych

Największym wyzwaniem współczesnych inżynierów kwantowych jest umieszczenie jak największej liczby logicznych kubitów w jednym układzie, bez jednoczesnego zwiększania podatności systemu na zakłócenia środowiskowe [4]. Problem ten jest jednym z kluczowych ograniczeń skalowania komputerów kwantowych.

Obecnie istnieje wiele proponowanych technologii realizacji kubitów, jednak cztery z nich dominują pod względem dojrzałości eksperymentalnej i poziomu rozwoju: kubity nadprzewodzące, uwięzione jony, atomy neutralne oraz kubity fotonowe [8, 9, 10, 11]. Oprócz nich intensywnie rozwijane są również inne podejścia, takie jak kubity oparte na półprzewodnikach, kubity topologiczne [7], kubity diamentowe [1], systemy typu quantum annealing [2] oraz tzw. cat qubits [3]. W niniejszej pracy zostaną jednak omówione pierwsze cztery najbardziej dojrzałe i szeroko badane architektury.

Kubity nadprzewodzące stanowią jedną z najczęściej stosowanych obecnie technologii. Wykorzystują one materiały nadprzewodzące schładzane do bardzo niskich temperatur, bliskich zeru absolutnemu. W takich warunkach opór elektryczny zanika, co umożliwia przepływ prądu bez strat energetycznych. Dzięki temu możliwe jest tworzenie i kontrolowanie makroskopowych stanów kwantowych, które pełnią rolę kubitów [11]. W praktyce są to układy szczególnie wrażliwe na zakłócenia elektromagnetyczne i defekty materiałowe.

Drugą istotną platformą są systemy oparte na uwięzionych jonach. W tym podejściu kubitami są pojedyncze jony (czyli naładowane atomy), utrzymywane w przestrzeni za pomocą pól elektromagnetycznych w warunkach próżni. Informacja kwantowa kodowana jest w stanach energetycznych tych jonów [8]. Systemy tego typu charakteryzują

się bardzo wysoką precyzją operacji kwantowych, jednak ich skalowanie pozostaje technicznie wymagające.

Kolejną kategorią są komputery kwantowe oparte na atomach neutralnych. W tym podejściu wykorzystuje się pojedyncze atomy pozbawione ładunku elektrycznego, które są utrzymywane w tzw. pułapkach optycznych tworzonych przez wiązki laserowe. Tego typu architektura nie wymaga ekstremalnego chłodzenia w takim stopniu jak układy nadprzewodzące, ani silnych pól elektromagnetycznych stosowanych w pułapkach jonowych [9]. Z tego powodu jest to jedna z najbardziej obiecujących ścieżek skalowania systemów kwantowych.

Ostatnią z omawianych technologii są komputery fotonowe, w których informacja kwantowa kodowana jest w pojedynczych fotonach. Układy te wykorzystują elementy optyczne, takie jak interferometry oraz światłowody, do manipulacji stanami kwantowymi światła. Ponieważ fotony bardzo słabo oddziałują z otoczeniem, systemy te są z natury mniej podatne na część typów zakłóceń, co stanowi ich istotną zaletę [10].

Wszystkie opisane podejścia mają jednak wspólną cechę: ich rozwój ograniczany jest przez szumy oraz trudności skalowania układów wielokubitowych (problemy te szerzej omawiane w sekcji 4). W praktyce oznacza to, że wybór architektury jest zawsze kompromisem pomiędzy precyzją operacji, łatwością skalowania oraz odpornością na błędy [4, 8, 9, 10, 11].

4. Zjawiska fizyczne i źródła błędów

W praktyce kubit jest obiektem fizycznym, który nieustannie oddziałuje ze swoim otoczeniem. To właśnie te oddziaływania są głównym źródłem błędów ograniczających możliwości współczesnych urządzeń NISQ [4].

Jednym z podstawowych źródeł problemów są błędy bramek kwantowych. Żadna rzeczywista operacja nie jest wykonywana idealnie. Każdy impuls mikrofalowy, sygnał sterujący lub impuls laserowy wnosi pewien błąd, przez co rzeczywista operacja różni się nieznacznie od tej zaplanowanej przez algorytm.

Dodatkowym wyzwaniem są błędy pomiaru. Odczyt stanu kubitu sam w sobie jest procesem fizycznym, który również jest obarczony niepewnością [13]. W rezultacie urządzenie może błędnie zinterpretować stan kubitu nawet wtedy, gdy wszystkie wcześniejsze operacje zostały wykonane poprawnie.

Szczególnie problematyczne jest to, że błędy kwantowe mają charakter kumulacyjny. Wraz ze wzrostem liczby kubitów i wykonywanych operacji rośnie prawdopodobieństwo pojawienia się zakłóceń [15]. Oznacza to, że zwiększenie rozmiaru procesora nie prowadzi automatycznie do zwiększenia jego użyteczności a czasem jest nawet odwrotnie. W pewnym momencie liczba błędów może rosnąć szybciej niż zdolność układu do wykonywania poprawnych obliczeń.

Właśnie dlatego współczesna inżynieria kwantowa koncentruje się nie tylko na budowie coraz większych procesorów, ale również na redukcji częstości występowania

błędów [4]. Bez rozwiązania tych problemów stworzenie dużych, uniwersalnych komputerów kwantowych pozostanie niemożliwe.

5. Korekcja błędów kwantowych

Skoro błędy kwantowe są nieuniknioną konsekwencją oddziaływania kubitów z otoczeniem, naturalnie pojawia się pytanie, czy można je korygować podobnie jak błędy występujące w klasycznych komputerach [4]. W przypadku systemów klasycznych problem jest stosunkowo prosty. Jeżeli bit przyjmuje wartość 0 lub 1, wystarczy przechowywać kilka kopii tej samej informacji i okresowo sprawdzać zgodność pomiędzy nimi. W razie wykrycia niezgodności można przyjąć wartość większościową i w ten sposób odzyskać poprawną informację [13].

W świecie kwantowym sytuacja jest znacznie bardziej skomplikowana. Podstawowym ograniczeniem jest tzw. twierdzenie o zakazie klonowania (ang. No Cloning Theorem), zgodnie z którym nie istnieje operacja pozwalająca na utworzenie idealnej kopii nieznanego stanu kwantowego [18]. Oznacza to, że klasyczne podejście polegające na wielokrotnym kopiowaniu danych nie może zostać bezpośrednio zastosowane do kubitów.

Gdyby po każdym kroku algorytmu próbować sprawdzić stan wszystkich kubitów, obliczenie kwantowe zostałoby natychmiast przerwane [13]. Korekcja błędów kwantowych musi więc działać bez bezpośredniego odczytywania przechowywanej informacji. Rozwiązaniem tego problemu jest kodowanie jednego kubitów logicznego w większej liczbie kubitów fizycznych. Informacja nie jest przechowywana w pojedynczym elemencie układu, lecz rozkładana pomiędzy wieloma kubitami za pomocą splątania [13]. Dzięki temu możliwe staje się wykrywanie błędów bez poznawania właściwej wartości przechowywanej informacji kwantowej.

Współczesne systemy wykorzystują bardziej zaawansowane schematy kodowania. Szczególnie duże zainteresowanie budzą tzw. kody powierzchniowe (ang. surface codes), które są obecnie uznawane za jedną z najbardziej obiecujących metod budowy komputerów kwantowych odpornych na błędy [20]. Ich zaletą jest stosunkowo wysoka tolerancja na zakłócenia oraz możliwość implementacji na wielu współczesnych architekturach sprzętowych.

Należy jednak pamiętać, że korekcja błędów kwantowych wiąże się z ogromnym narzutem sprzętowym. Jeden kubit logiczny wymaga zazwyczaj wykorzystania wielu kubitów fizycznych [4, 20]. W zależności od zastosowanego kodu oraz jakości sprzętu liczba ta może wynosić od kilkudziesięciu do nawet kilku tysięcy kubitów fizycznych na jeden stabilny kubit logiczny.

To właśnie ten narzut stanowi obecnie jedno z największych ograniczeń rozwoju komputerów kwantowych. Współczesne procesory NISQ dysponują setkami lub tysiącami kubitów fizycznych, jednak po uwzględnieniu mechanizmów korekcji błędów liczba dostępnych kubitów logicznych jest nadal bardzo niewielka. Przykładowo, procesor

dysponujący tysiącem kubitów fizycznych może realizować zaledwie kilka kubitów logicznych przy zastosowaniu kodów powierzchniowych [16]. Z tego powodu większość obecnych urządzeń nie implementuje jeszcze pełnej korekcji błędów kwantowych, a zamiast tego wykorzystuje różnego rodzaju techniki ograniczania wpływu błędów (ang. error mitigation) [4].

Można więc powiedzieć, że korekcja błędów kwantowych jest jednym z kluczowych warunków koniecznych do osiągnięcia praktycznych, uniwersalnych komputerów kwantowych [4, 20]. Dopiero stworzenie dużej liczby stabilnych kubitów logicznych pozwoli na wykonywanie długich i złożonych obliczeń bez utraty informacji kwantowej.

6. Ograniczenia skalowania systemów NISQ

Naturalnym kierunkiem rozwoju komputerów kwantowych wydaje się zwiększanie liczby dostępnych kubitów. W przeciwieństwie do klasycznych procesorów wzrost liczby elementów obliczeniowych nie przekłada się jednak w prosty sposób na wzrost możliwości systemu. W przypadku urządzeń NISQ liczba kubitów jest tylko jednym z parametrów określających jakość komputera kwantowego. Równie istotne są dokładność bramek kwantowych, jakość pomiarów oraz poziom szumów występujących w układzie [4].

W praktyce każdy dodatkowy kubit zwiększa złożoność całego systemu. Konieczne staje się dostarczenie większej liczby sygnałów sterujących, zapewnienie odpowiedniego chłodzenia, synchronizacji oraz izolacji od zakłóceń środowiskowych. Problem ten jest szczególnie widoczny w przypadku kubitów nadprzewodzących, gdzie każdy element układu wymaga połączenia z rozbudowaną elektroniką sterującą pracującą w temperaturach bliskich zeru absolutnemu [11].

Dodatkową trudność stanowi fakt, że wzrost liczby kubitów zwykle prowadzi również do wzrostu liczby potencjalnych źródeł błędów. Nawet jeśli pojedynczy kubit działa z bardzo wysoką dokładnością, prawdopodobieństwo wystąpienia błędu rośnie wraz z liczbą wykonywanych operacji. Oznacza to, że duży procesor może w praktyce generować więcej błędów niż jest w stanie wykorzystać do poprawnych obliczeń [20].

Istotnym problemem jest również tzw. połączenie wszystkich ze wszystkimi (ang. all-to-all connectivity). W wielu algorytmach konieczne jest wykonywanie operacji pomiędzy odległymi kubitami. W rzeczywistych architekturach większość kubitów może jednak komunikować się jedynie z najbliższymi sąsiadami. Wymusza to wykonywanie dodatkowych operacji pośrednich, które zwiększają czas obliczeń oraz prawdopodobieństwo wystąpienia błędów [11].

Kolejnym ograniczeniem jest sama korekcja błędów kwantowych. Jak wspomniano w poprzedniej sekcji, stabilny kubit logiczny wymaga wykorzystania wielu kubitów fizycznych. Oznacza to, że nawet procesor zawierający kilka tysięcy kubitów fizycznych może być zdolny do utworzenia jedynie niewielkiej liczby kubitów logicznych.

W konsekwencji współczesne urządzenia NISQ znajdują się poniżej progu umożliwiającego budowę w pełni odpornych na błędy komputerów kwantowych [20].

Problem ten dobrze ilustrują współczesne rekordy liczby kubitów. W ostatnich latach zaprezentowano eksperymentalne układy zawierające tysiące kubitów fizycznych [6]. Sam wzrost liczby elementów nie oznacza jednak automatycznie proporcjonalnego wzrostu mocy obliczeniowej. Znacznie ważniejszym parametrem staje się bowiem liczba dostępnych kubitów logicznych oraz możliwość wykonywania długich sekwencji operacji bez utraty informacji kwantowej.

Z tego powodu coraz częściej podkreśla się, że przyszłość komputerów kwantowych zależy nie tylko od zwiększania liczby kubitów, ale również od poprawy jakości ich działania. W praktyce oznacza to zmniejszanie błędów bramek, rozwój skuteczniejszych metod korekcji błędów oraz projektowanie architektur umożliwiających łatwiejsze skalowanie.

Można więc powiedzieć, że współczesna era NISQ jest okresem przejściowym pomiędzy pierwszymi działającymi procesorami kwantowymi a przyszłymi komputerami odpornymi na błędy. Choć liczba kubitów stale rośnie, największym wyzwaniem pozostaje obecnie nie samo budowanie większych układów, lecz utrzymanie ich jakości na poziomie umożliwiającym wykonywanie użytecznych obliczeń kwantowych.

7. Kryptografia a problem Q-Day

Jednym z najczęściej dyskutowanych zastosowań komputerów kwantowych jest ich potencjalny wpływ na współczesną kryptografię [21]. Większość obecnie stosowanych systemów bezpieczeństwa cyfrowego opiera się na problemach matematycznych uznawanych za bardzo trudne do rozwiązania przy użyciu klasycznych komputerów. Dotyczy to między innymi algorytmów RSA, Diffie-Hellmana oraz kryptografii opartej na krzywych eliptycznych (ECC), które stanowią fundament bezpieczeństwa współczesnego Internetu [13].

Bezpieczeństwo tych systemów wynika z faktu, że pewne operacje matematyczne są łatwe do wykonania, ale niezwykle trudne do odwrócenia. Przykładowo, pomnożenie dwóch bardzo dużych liczb pierwszych jest zadaniem prostym, natomiast odnalezienie tych liczb na podstawie samego wyniku stanowi problem obliczeniowo kosztowny dla klasycznych komputerów. Właśnie na tej asymetrii opiera się bezpieczeństwo algorytmu RSA.

Sytuacja zmienia się jednak w obecności wystarczająco dużego komputera kwantowego. W 1994 roku Peter Shor zaproponował algorytm umożliwiający efektywne rozkładanie liczb na czynniki pierwsze oraz rozwiązywanie problemu logarytmu dyskretnego w czasie wielomianowym [21]. Oznacza to, że komputer kwantowy dysponujący odpowiednią liczbą stabilnych kubitów logicznych mógłby potencjalnie złamać znaczną część współcześnie wykorzystywanych systemów kryptografii asymetrycznej.

Hipotetyczny moment, w którym stanie się to możliwe, określany jest często mianem Q-Day. Termin ten nie posiada jednej ścisłej definicji, jednak najczęściej oznacza moment osiągnięcia przez komputery kwantowe zdolności do praktycznego łamania powszechnie stosowanych systemów kryptograficznych [22].

Warto podkreślić, że obecne urządzenia NISQ są bardzo dalekie od osiągnięcia tego celu. Chociaż współczesne procesory kwantowe dysponują setkami lub nawet tysiącami kubitów fizycznych, skuteczne uruchomienie algorytmu Shora dla kluczy kryptograficznych stosowanych w praktyce wymagałoby znacznie większej liczby stabilnych kubitów logicznych oraz pełnej korekcji błędów kwantowych [4]. Z tego powodu eksperci są zgodni, że współczesne komputery kwantowe nie stanowią bezpośredniego zagrożenia dla bezpieczeństwa powszechnie wykorzystywanych systemów szyfrowania.

Pośrednie zagrożenie istnieje już dziś. W scenariuszu Harvest Now, Decrypt Later [22] archiwizowane dane zostaną odszyfrowane po powstaniu wystarczająco mocnych komputerów kwantowych.

W odpowiedzi na to zagrożenie rozwijana jest kryptografia postkwantowa (ang. Post-Quantum Cryptography, PQC) [23]. Jej celem jest stworzenie algorytmów odpornych zarówno na ataki klasyczne, jak i kwantowe. W przeciwieństwie do kryptografii kwantowej nie wymaga ona wykorzystania komputerów kwantowych, lecz opiera się na nowych problemach matematycznych, dla których nie są znane skuteczne algorytmy kwantowe.

Prace nad standaryzacją takich rozwiązań prowadzi między innymi amerykański Narodowy Instytut Standaryzacji i Technologii (NIST) [23]. W ostatnich latach wybrano pierwsze standardy kryptografii postkwantowej przeznaczone do zastąpienia obecnych algorytmów asymetrycznych [23]. Proces ten jest uznawany za jeden z największych projektów modernizacji infrastruktury kryptograficznej w historii Internetu [23].

Paradoksalnie największy wpływ komputerów kwantowych na bezpieczeństwo cyfrowe jest widoczny już dziś, mimo że nie istnieją jeszcze maszyny zdolne do praktycznego łamania współczesnej kryptografii. Sama perspektywa osiągnięcia Q Day zmusza instytucje rządowe, firmy technologiczne oraz środowiska naukowe do przygotowywania nowych standardów bezpieczeństwa na wiele lat przed pojawieniem się odpowiednio zaawansowanych komputerów kwantowych.

Można zatem stwierdzić, że Q-Day nie jest wyłącznie problemem technologicznym. Jest również wyzwaniem organizacyjnym, ekonomicznym i społecznym, wymagającym długoterminowego planowania oraz stopniowej migracji do systemów odpornych na przyszłe zagrożenia kwantowe [22].

8. Nauczanie informatyki kwantowej w szkole średniej

Dynamiczny rozwój technologii kwantowych powoduje wzrost zainteresowania zarówno środowisk naukowych, jak i przemysłu zagadnieniami związanymi z obliczeniami kwantowymi. Jak pokazano w poprzednich sekcjach, współczesne komputery

kwantowe znajdują się obecnie w erze NISQ, charakteryzującej się szybkim wzrostem liczby kubitów oraz intensywnym rozwojem nowych architektur sprzętowych [4]. Powstaje zatem pytanie, czy wraz z rozwojem technologii kwantowych powinno zmieniać się również kształcenie przyszłych informatyków.

Intuicja podpowiada że odpowiedź jest negatywna. Informatyka kwantowa opiera się bowiem na mechanice kwantowej, której formalny opis wymaga wykorzystania algebry liniowej, rachunku macierzowego oraz liczb zespolonych [13]. Są to zagadnienia wykraczające poza standardowy program nauczania szkoły średniej. Można więc odnieść wrażenie, że nauczanie informatyki kwantowej powinno pozostać domeną studiów wyższych.

Dokładniejsza analiza prowadzi jednak do innych wniosków. Współczesna edukacja nie wymaga od uczniów pełnego formalnego opisu wielu zjawisk naukowych. Przykładowo podstawowe idee teorii względności czy fizyki atomowej są omawiane jeszcze przed rozpoczęciem studiów. Podobne podejście można zastosować do informatyki kwantowej. Pojęcia takie jak kubit, superpozycja czy splątanie mogą być przedstawiane intuicyjnie, bez konieczności wprowadzania pełnego aparatu matematycznego mechaniki kwantowej.

Szczególnie użyteczne wydaje się porównanie klasycznego bitu z kubitami. Uczeń posiadający podstawową wiedzę z zakresu informatyki i rachunku prawdopodobieństwa jest w stanie zrozumieć, że kubit różni się od klasycznego bitu możliwością występowania w superpozycji stanów [13]. Analogicznie pojęcie splątania może zostać przedstawione jako szczególny rodzaj zależności pomiędzy układami kwantowymi, bez konieczności formalnego opisu stanów wielokubitowych.

Nie wszystkie zagadnienia informatyki kwantowej nadają się jednak do nauczania na poziomie szkoły średniej. Zaawansowane algorytmy, takie jak algorytm Shora wykorzystywany do faktoryzacji liczb [21], wymagają znajomości pojęć matematycznych znacznie wykraczających poza program liceum. Możliwe wydaje się natomiast przedstawienie idei przewagi obliczeń kwantowych nad klasycznymi bez analizowania wszystkich szczegółów matematycznych. W takim ujęciu celem nauczania byłoby zrozumienie zasad działania komputerów kwantowych, a nie samodzielne projektowanie algorytmów.

Argumentem przemawiającym za wprowadzeniem elementów edukacji kwantowej jest również rosnące znaczenie zagadnień związanych z bezpieczeństwem cyfrowym. Jak wskazuje Mosca [22], perspektywa pojawienia się komputerów kwantowych zdolnych do łamania współczesnych systemów kryptograficznych już dziś wpływa na rozwój kryptografii postkwantowej. Oznacza to, że przyszli informatycy będą musieli rozumieć podstawowe konsekwencje rozwoju technologii kwantowych niezależnie od tego, czy będą bezpośrednio zajmować się obliczeniami kwantowymi.

Istotną zaletą edukacji kwantowej jest również możliwość wykorzystania symulatorów komputerowych. W przeciwieństwie do wielu zaawansowanych laboratoriów

fizycznych nauczanie podstaw obliczeń kwantowych nie wymaga dostępu do rzeczywistego procesora kwantowego. Uczniowie mogą eksperymentować z prostymi obwodami kwantowymi przy użyciu klasycznych komputerów, obserwując działanie podstawowych bramek oraz wpływ pomiaru na stan kubitu.

Należy jednak zauważyć, że wdrożenie takich treści do programu nauczania wiązałoby się z szeregiem wyzwań. Informatyka kwantowa znajduje się na styku fizyki, matematyki oraz informatyki, co oznacza konieczność odpowiedniego przygotowania nauczycieli. Dodatkowym problemem jest ograniczona liczba materiałów dydaktycznych opracowanych specjalnie z myślą o edukacji szkolnej.

Wszystko wskazuje na to, że najbardziej prawdopodobnym scenariuszem rozwoju edukacji nie jest utworzenie odrębnego przedmiotu poświęconego komputerom kwantowym, lecz stopniowe wprowadzanie wybranych zagadnień do istniejących kursów informatyki i fizyki. Podejście takie pozostaje zgodne z kierunkiem rozwoju współczesnej informatyki, w której coraz większą rolę odgrywają zagadnienia wykraczające poza klasyczny model obliczeń.

Można zatem przypuszczać, że podobnie jak obecnie uczniowie poznają podstawy sztucznej inteligencji, kryptografii czy sieci komputerowych, tak w przyszłości podstawowe pojęcia związane z informatyką kwantową staną się naturalnym elementem kształcenia informatycznego. Nie będzie to oznaczało nauczania pełnej mechaniki kwantowej, lecz raczej przygotowanie uczniów do funkcjonowania w świecie, w którym technologie kwantowe mogą odgrywać coraz większą rolę.

9. Podsumowanie i perspektywy rozwoju

Rozwój komputerów kwantowych znajduje się obecnie w fazie przejściowej, określanej jako era NISQ. Jak omówiono w poprzednich sekcjach, zastosowania współczesnych urządzeń kwantowych pozostają silnie ograniczone przez szumy oraz błędy operacyjne [4].

Z jednej strony obserwujemy szybki postęp technologiczny, który obejmuje zwiększanie liczby kubitów fizycznych oraz rozwój różnych architektur sprzętowych, takich jak kubity nadprzewodzące, uwięzione jony, atomy neutralne czy układy fotonowe. Każda z tych technologii oferuje inne kompromisy pomiędzy skalowalnością, precyzją operacji i odpornością na zakłócenia [8, 9, 10, 11].

Z drugiej strony wszystkie obecne systemy napotykają fundamentalne ograniczenia wynikające z fizyki układów kwantowych. Błędy bramek oraz niedoskonałości pomiarów sprawiają, że zwiększanie liczby kubitów nie przekłada się liniowo na wzrost mocy obliczeniowej. W praktyce oznacza to, że współczesne procesory kwantowe pozostają daleko od stanu, w którym możliwe byłoby niezawodne wykonywanie długich algorytmów kwantowych [20].

Kluczowym krokiem w kierunku pełnoskalowych komputerów kwantowych pozostaje skuteczna korekcja błędów oraz budowa stabilnych kubitów logicznych. Dopiero

systemy zdolne do długotrwałego utrzymywania informacji kwantowej mogą stać się podstawą uniwersalnych obliczeń kwantowych. Wymaga to jednak znaczącego zwiększenia liczby kubitów fizycznych oraz poprawy ich jakości, co nadal stanowi jedno z największych wyzwań współczesnej inżynierii kwantowej.

W perspektywie krótko i średnioterminowej najbardziej prawdopodobnym scenariuszem rozwoju są tzw. algorytmy hybrydowe, w których część obliczeń wykonywana jest przez komputery klasyczne, a część przez układy kwantowe. Takie podejście pozwala wykorzystać ograniczone możliwości systemów NISQ bez konieczności pełnej korekcji błędów. Długoterminowo oczekuje się natomiast przejścia do tzw. komputerów kwantowych odpornych na błędy (ang. *fault-tolerant quantum computers*). Ich realizacja będzie wymagała zarówno dalszego rozwoju technologii sprzętowych, jak i udoskonalenia metod kodowania informacji kwantowej [4].

Na tym tle coraz wyraźniej widać, że rozwój technologii kwantowych nie dotyczy wyłącznie warstwy inżynierskiej, ale również edukacyjnej i społecznej. Jak pokazano w jednym z wcześniejszych rozdziałów, podstawowe pojęcia informatyki kwantowej, takie jak kubit, superpozycja czy splątanie, mogą być wprowadzane już na poziomie szkoły średniej w sposób intuicyjny, bez konieczności pełnego formalizmu matematycznego [17].

Taki kierunek ma istotne znaczenie praktyczne. Wraz z rozwojem technologii kwantowych rośnie bowiem zapotrzebowanie na specjalistów, którzy nie tylko rozumieją fizyczne podstawy działania takich systemów, ale również potrafią myśleć w kategoriach hybrydowych modeli obliczeń. Wczesne oswojenie uczniów z podstawowymi pojęciami może w przyszłości ułatwić im wejście w bardziej zaawansowane zagadnienia inżynierii kwantowej [12].

Jednocześnie należy podkreślić, że edukacja kwantowa na poziomie szkolnym nie powinna polegać na nauczaniu zaawansowanej mechaniki kwantowej, lecz raczej na budowaniu intuicji dotyczącej różnic pomiędzy klasycznym a kwantowym modelem informacji. W tym sensie pełni ona rolę analogiczną do wprowadzenia podstaw sztucznej inteligencji czy kryptografii w edukacji ogólnej.

Podsumowując, obecna era NISQ nie jest końcem rozwoju komputerów kwantowych, lecz etapem pośrednim pomiędzy teorią a w pełni praktycznymi zastosowaniami. Choć współczesne urządzenia wciąż mają ograniczoną użyteczność, stanowią one istotny krok w kierunku przyszłych systemów obliczeniowych, które mogą fundamentalnie zmienić sposób przetwarzania informacji, a także sposób jej nauczania i rozumienia.

Literatura

1. D. Awschalom, R. Hanson, J. Wrachtrup, B. B. Zhou, Quantum technologies with diamondspin systems, *Nature Photonics*, vol. 12, 2018.

2. M. W. Johnson et al., Quantum annealing with manufactured spins, *Nature*, vol. 473, 2011.
3. M. Mirrahimi et al., Dynamically protected cat-qubits, *New Journal of Physics*, vol. 16, 2014.
4. J. Preskill, Quantum Computing in the NISQ Era and Beyond, *Quantum*, vol. 2, no. 79, 2018, doi: 10.22331/q-2018-08-06-79.
5. National Academies of Sciences, Engineering, and Medicine. (2019). *Quantum Computing: Progress and Prospects*. The National Academies Press.
6. California Institute of Technology, Caltech Team Sets Record with 6,100-Qubit Array, 2025, <https://www.caltech.edu/about/news/caltech-team-sets-record-with-6100-qubit-array>
7. C. Nayak et al., Non-Abelian Anyons and Topological Quantum Computation, *Reviews of Modern Physics*, vol. 80, 2008.
8. H. Häner et al., Quantum Computing with Trapped Ions, *Physics Reports*, vol. 469, 2008.
9. L. Henriot et al., Quantum Computing with Neutral Atoms, *Quantum*, vol. 4, 2020.
10. J. Romero, G. Milburn, Photonic Quantum Computing, *AVS Quantum Science*, vol. 3, 2021.
11. J. Krantz et al., A quantum engineer's guide to superconducting qubits, *Applied Physics Reviews*, 6, 021318 (2019).
12. M. F. J. Fox, B. L. Z. Zwickl, Introducing quantum concepts in secondary school: A diagnostic study, *Physical Review Physics Education Research*, vol. 19, no. 1, 010118, 2023.
13. M. A. Nielsen, I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2010.
14. P. A. M. Dirac, *The Principles of Quantum Mechanics*, Oxford University Press, 1981.11
15. W. H. Zurek, Decoherence, Einselection, and the Quantum Origins of the Classical, *Reviews of Modern Physics*, vol. 75, 2003.
16. Gidney, C., & Ekerå, M. (2021). How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits. *Quantum*, 5, 433.
17. S. Atkinson, J. et al., Quantum education and outreach: teaching quantum concepts at preuniversity level, *arXiv preprint*, 2021.
18. W. K. Wootters, W. H. Zurek, A Single Quantum Cannot be Cloned, *Nature*, vol. 299, pp.802-803, 1982.

19. Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, 549(7671), 188–194.
20. A. G. Fowler, M. Mariantoni, J. M. Martinis, A. N. Cleland, Surface Codes: Towards Practical Large-Scale Quantum Computation, *Physical Review A*, vol. 86, 032324, 2012.
21. P. W. Shor, Algorithms for Quantum Computation: Discrete Logarithms and Factoring, *Proceedings of the 35th Annual Symposium on Foundations of Computer Science*, 1994.
22. M. Mosca, Cybersecurity in an Era with Quantum Computers: Will We Be Ready?, *IEEE Security & Privacy*, vol. 16, no. 5, pp. 38–41, 2018.
23. National Institute of Standards and Technology, Post-Quantum Cryptography Standardization, <https://www.nist.gov/pqcrypto>