ISSN 1998-7927(print) ISSN 2664-6498 (online)

DOI: https://doi.org/10.33216/1998-7927-2026-301-3-25-32

УДК 004.383.8:004.421

ПОРІВНЯЛЬНИЙ АНАЛІЗ КВАНТОВИХ СХЕМ ВІДНІМАННЯ В БАЗИСІ СУЧАСНИХ КВАНТОВИХ ПРОЦЕСОРІВ

Полупан Ю.В.

COMPARATIVE ANALYSIS OF QUANTUM SUBTRACTION CIRCUITS IN THE BASIS OF MODERN QUANTUM PROCESSORS

Polupan Yu.V.

У роботі досліджено шість квантових схем віднімачів, реалізованих у середовищі Qiskit: Out-of-place ripple-borrow subtractor, In-place ripple-borrow subtractor, Cuccaro ripple-carry subtractor, Parallel Carry-lookahead subtractor, Parallel-prefix Kogge-Stone subtractor та QFT-based subtractor за підходом Draper. Метою дослідження є порівняння схем за кількістю кубітів, кількістю гейтів, глибиною, CNOT-count, CNOT-depth, T-count і T-depth після транспіляції до базису {CX, T, T†, H, X, S, S†}. Показано, що для трирозрядних операндів найменшу кількість кубітів мають In-place ripple-borrow та QFT-based схеми, тоді як найменшу транспільовану глибину демонструє Parallel Carry-lookahead subtractor. QFT-based схема має малу кількість CNOT-гейтів, однак після розкладання контрольованих фазових зсувів CP у Clifford+T-базис її T-вартість стає на кілька порядків більшою за інші схеми. Отримані результати підтверджують, що вибір архітектури віднімача залежить від цільової моделі обчислень: для fault-tolerant Clifford+T-реалізації перевагу мають схеми з контрольованою T-складністю, тоді як QFT-підхід доцільніше оцінювати в нативних фазових базисах.

Загалом результати показують, що для малих розрядностей і Clifford+T-орієнтованої реалізації найбільш збалансованим вибором є Parallel Carry-lookahead subtractor, тоді як Ripple-borrow схеми залишаються привабливими за умови дефіциту кубітів. QFT-based підхід потребує окремого аналізу в апаратних моделях, де фазові зсуви є дешевшими або підтримуються нативно.

З навчально-методичного погляду такий аналіз є важливим для формування у студентів практичного розуміння архітектурної різноманітності квантових арифметичних схем. Порівняння різних типів віднімачів показує, що одна й та сама операція може бути реалізована через принципово різні підходи, які по-різному проявляють себе на логічному та фізичному рівнях. Це дає змогу студентам усвідомити, що вибір алгоритму або схемної реалізації залежить не лише від математичної постановки задачі, а й від цільової квантової архітектури, нативного набору гейтів, кількості доступних кубітів і вимог до fault-tolerant виконання.

Ключові слова: *квантові обчислення, квантова арифметика, квантове віднімання, віднімач, Qiskit, Clifford+T, ripple-borrow, carry-lookahead, Kogge-Stone, QFT, Draper adder.*

1. Вступ. Квантові обчислення ґрунтуються на використанні суперпозиції, унітарної еволюції та заплутаності квантових станів, що дає змогу будувати алгоритми, принципово відмінні від класичних [1, 2]. Одним із базових напрямів розвитку квантових алгоритмів є квантова арифметика, оскільки операції додавання, віднімання, множення та модульного піднесення до степеня використовуються в алгоритмах факторизації, пошуку, симуляції фізичних систем і криптоаналітичних застосуваннях [2, 3, 4].

Водночас дослідження та порівняння схем квантових арифметичних пристроїв має важливе навчально-методичне значення, оскільки такі схеми є наочними прикладами реалізації унітарних перетворень, роботи з квантовими регістрами, допоміжними кубітами та оборотними логічними елементами. Зокрема, аналіз різних типів квантових віднімачів може бути використаний в освітньому процесі підготовки здобувачів другого (магістерського) рівня вищої освіти, які вивчають освітній компонент «Теорія квантової інформації та обчислень» освітньої програми «Інженерія

квантового програмного забезпечення», як засіб формування практичного розуміння принципів побудови квантових обчислювальних схем.

Операція віднімання є особливо важливою, оскільки вона може реалізовуватися як самостійна оборотна арифметична процедура або через додавання числа у формі доповнення до двох. У квантових схемах така операція повинна бути оборотною, а тому потребує уважного керування допоміжними кубітами, проміжними переносами або позиками та процедурою очищення тимчасових регістрів. Класичні ідеї ripple-carry, carry-lookahead та parallel-prefix арифметики мають квантові аналоги, однак їхня ефективність істотно залежить від набору елементарних гейтів і вартості декомпозиції Toffoli- та фазових операцій [5, 6, 7, 8].

У сучасних fault-tolerant моделях важливу роль відіграє Clifford+T-базис. Clifford-гейти, зокрема {CX, H, X, S, $S^{\dagger}$} зазвичай вважаються дешевшими у корекції помилок, тоді як T-гейти потребують складніших процедур магічної дистиляції. Тому T-count і T-depth є критичними метриками складності квантових арифметичних схем [2, 9]. Водночас QFT-based арифметика, започаткована в роботах Draper, дозволяє виконувати додавання й віднімання у фур'є-базисі через контрольовані фазові зсуви [10, 11]. Такий підхід може бути компактним на абстрактному рівні, але його ефективність суттєво залежить від того, чи доступні контрольовані фазові гейти нативно.

Метою цієї роботи є експериментальне порівняння шести квантових схем віднімання для трирозрядних операндів, реалізованих у Qiskit [12-14], із подальшою транспіляцією до Clifford+T-базису, а також висвітлення навчально-методичного значення такого аналізу. Для студентів, які вивчають квантові обчислення, таке порівняння є корисним, оскільки дає змогу побачити, що ефективність тієї чи іншої схеми може істотно змінюватися залежно від фізичної реалізації обчислювального пристрою.

2. Теоретичні основи квантового віднімання Для двох n-бітових чисел A і B віднімання може бути представлене як

$$D = A - B.$$

У класичній двійковій арифметиці ця операція може виконуватися або через послідовне поширення позики, або через додавання доповнення до двох:

$$A - B = A + (\bar{B} + 1).$$

У квантовій схемотехніці обидва підходи повинні бути реалізовані оборотно. Це означає, що вхідна інформація не може бути безповоротно стерта, а всі проміжні значення мають або зберігатися в окремих регістрах, або бути очищені через uncomputation.

Ripple-borrow схеми віднімання поширюють позику від молодших бітів до старших. Їх перевагою є відносно мала кількість кубітів і проста структура, але глибина зростає лінійно з розрядністю. Ripple-carry підхід Cuccaro, первинно запропонований для додавання, може бути адаптований до віднімання через перетворення операндів і використання логіки переносу [6]. Parallel Carry-lookahead схеми намагаються зменшити глибину шляхом паралельного обчислення сигналів генерації та поширення переносу або позики [7]. Parallel-prefix схеми, зокрема Kogge–Stone, використовують префіксну мережу для швидкого поширення інформації про перенос, що в класичній арифметиці забезпечує логарифмічну глибину [8].

QFT-based підхід використовує квантове перетворення Фур'є, після якого арифметична операція виконується за допомогою контрольованих фазових зсувів CP. Draper показав, що додавання у фур'є-базисі може бути реалізоване через контрольовані фазові зсуви [11]. Віднімання може бути побудоване аналогічно, змінюючи знаки фаз або використовуючи доповнення до двох [10].

3. Методика дослідження. Для порівняльного аналізу було обрано шість схем квантового віднімання, які репрезентують основні архітектурні підходи до побудови арифметичних квантових модулів: послідовне поширення позики, використання переносу через доповнення до двох, паралельне передбачення позики, parallel-prefix обчислення та QFT-based арифметику. Такий вибір дає змогу порівняти не лише окремі реалізації, а й різні принципи організації квантового віднімання. Схеми, що були проаналізовані:

1) **Out-of-place ripple-borrow subtractor** та **in-place ripple-borrow subtractor**, оскільки ripple-borrow схеми є найбільш прямими квантовими аналогіями класичного двійкового віднімання з послідовним поширенням позики. Ці дві схеми дозволяють

окремо оцінити компроміс між кількістю кубітів і складністю обчислення. Out-of-place схема використовує додатковий регістр для результату, тому краще зберігає вхідні дані, але потребує більшої кількості кубітів. In-place схема записує результат у наявний регістр, що зменшує просторову складність, однак зазвичай ускладнює керування проміжними позиками та процедуру очищення допоміжних станів.

2) **Cuccaro ripple-carry subtractor**, оскільки ця схема є однією з найвідоміших і найчастіше використовуваних конструкцій квантової арифметики з лінійною глибиною та малою кількістю допоміжних кубітів [6]. Віднімання може бути реалізоване через модифікацію додавання, зокрема через інверсію одного з операндів і використання ідеї доповнення до двох. Тому така схема є природною контрольною точкою для порівняння з ripple-borrow реалізаціями та з більш паралельними архітектурами.

3) **Parallel Carry-lookahead subtractor** обрано для представлення схем, у яких зменшення глибини досягається за рахунок попереднього або паралельного обчислення сигналів генерації та поширення позики. Parallel Carry-lookahead підхід є класичною альтернативою ripple-структурам і має важливе значення для квантової арифметики, оскільки дозволяє зменшити залежність глибини від послідовного проходження переносу або позики [7]. Включення цієї схеми дає змогу перевірити, чи окуповується збільшення кількості допоміжних кубітів зменшенням T-depth, CNOT-depth і загальної глибини.

4) **Parallel-prefix Kogge–Stone subtractor** включено як приклад агресивнішої паралельної архітектури. Kogge–Stone мережі широко відомі в класичній схемотехніці як швидкі parallel-prefix adders з малою логарифмічною глибиною [8]. У контексті квантового віднімання така схема демонструє, як класична ідея паралельного префіксного обчислення може бути перенесена на оборотну логіку та реалізацію віднімання через доповнення до двох. Її включення важливе не тому, що вона очікувано найкраща для малого n=3, а тому, що вона показує інший край компромісу: більша кількість кубітів і Toffoli-подібних операцій в обмін на потенційно кращу масштабованість глибини для більших розрядностей.

5) **QFT-based Draper subtractor** обрано як представника принципово іншої моделі арифметики, у якій операція виконується не через булеву логіку переносу або позики, а у фур'є-базисі за допомогою контрольованих фазових обертань [10, 11]. Це дозволяє порівняти Toffoli/Clifford+T-орієнтовані схеми з QFT-based підходом. Така схема є особливо важливою для аналізу, оскільки на абстрактному рівні вона може мати компактну структуру й малу кількість CNOT-гейтів, але після транспіляції до дискретного Clifford+T-базису її вартість може різко зрости через декомпозицію фазових обертань.

Отже, обрані шість схем утворюють репрезентативний набір для порівняння. Вони охоплюють три основні класи квантового віднімання: класичні ripple-підходи, паралельні схеми на основі Parallel Carry-lookahead або prefix-мереж та альтернативну QFT-based модель. Завдяки цьому можна оцінити ключові компроміси між кількістю кубітів, глибиною, CNOT-вартістю та T-вартістю, а також визначити, які архітектури є доцільними для малих схем у Clifford+T-базисі.

Таким чином, у дослідженні розглянуто шість схем для операндів розрядності n=3:

1. Cuccaro ripple-carry subtractor, де результат A - B записується у регістр b.
2. Parallel carry-lookahead subtractor, де результат записується у регістр a.
3. Out-of-place ripple-borrow subtractor із окремим регістром різниці diff та окремим регістром bout, що використовується як допоміжні для зберігання проміжних бітів позики.
4. In-place ripple-borrow subtractor.
5. Parallel-prefix Kogge–Stone subtractor, що реалізує віднімання через паралельно-префіксну мережу для форми доповнення до двох.
6. QFT-based Draper subtractor.

Для кожної схеми оцінено два рівні складності: абстрактний рівень до транспіляції та рівень після транспіляції. Сучасні квантові пристрої умовно поділяють на NISQ-пристрої та fault-tolerant архітектури. NISQ-пристрої (Noisy Intermediate-Scale Quantum) мають від десятків до тисяч фізичних кубітів, однак характеризуються помітним рівнем шуму та, як правило, не використовують повноцінну квантову корекцію помилок. Тому схеми для таких пристроїв істотно обмежені за глибиною, оскільки похибки окремих операцій накопичуються під час обчислення.

Натомість fault-tolerant архітектури використовують квантові коди корекції помилок, зокрема surface code, у яких логічні кубіти кодуються багатьма фізичними кубітами

й захищаються від шуму. Це дає змогу виконувати значно глибші схеми, ніж на NISQ-пристроях, хоча й потребує суттєвих додаткових ресурсів.

Водночас практична вартість схеми залежить не лише від кількості гейтів після формальної транспіляції, а й від фізичної платформи. Наприклад, у trapped-ion системах характерними є висока зв'язність між кубітами та можливість ефективної реалізації фазових і контрольованих фазових гейтів. Натомість надпровідні системи (IBM, Google) мають обмежену зв'язність у вигляді двовимірної решітки, а їхніми native gates є CX та Rz, що робить їх природним середовищем для схем із великою кількістю CNOT-операцій. Фотонні системи (PsiQuantum) принципово відрізняються від інших: їхні native операції діють на фотони, а двокубітні взаємодії реалізуються імовірнісно, що суттєво впливає на структуру придатних схем.

Квантові віднімачі є арифметичними примітивами, що можуть входити до складу більших квантових алгоритмів, зокрема алгоритмів факторизації, квантової лінійної алгебри, моделювання фізичних систем і квантової хімії. Такі алгоритми мають практичний сенс насамперед у fault-tolerant режимі, де тривалі обчислення можуть виконуватися з контрольованим накопиченням помилок. У цьому контексті важливу роль відіграє Clifford+T-базис. Clifford-гейти {CX, H, X, S, $S^\dagger$) зазвичай вважаються дешевшими в реалізації з корекцією помилок, тоді як T- та $T^\dagger$-гейти потребують складніших процедур, зокрема підготовки магічних станів і магічної дистиляції. Тому в роботі для порівняння схем віднімачів проведено транспіляцію до Clifford+T-базису {CX, T, $T^\dagger$, H, X, S, $S^\dagger$), а основними метриками обрано кількість кубітів, загальну кількість гейтів, глибину схеми, CNOT-count, CNOT-depth, T-count і T-depth. Для QFT-based схем контрольовані фазові зсуви після транспіляції також зводяться до операцій обраного Clifford+T-базису, тому їхня вартість враховується через ті самі метрики, що й для інших схем.

4. Результати. Перед порівнянням метрик було проведено тестування коректності всіх реалізованих схем. Для різних вхідних комбінацій трирозрядних операндів A та B перевірялося, чи правильно схема формує результат віднімання та чи коректно очищує допоміжні регістри.

4.1. Абстрактний рівень

Таблиця 1

Значення метрик абстрактного рівня

№	Схема	Кубітів	Гейтів	Глибина	CNOT-depth / CP-depth
1	Cuccaro ripple-carry	10	28	19	18
2	Parallel Carry-lookahead	15	33	10	8
3	Out-of-place ripple-borrow	12	26	10	9
4	In-place ripple-borrow	8	23	12	10
5	Kogge–Stone	20	54	31	29
6	QFT-based Draper	8	33	17	CP-depth = 11, H-depth = 6

На абстрактному рівні найменшу кількість кубітів мають in-place ripple-borrow та QFT-based схеми: по 8 кубітів. Найменшу кількість гейтів має in-place ripple-borrow subtractor - 22 гейти. Найменшу глибину має out-of-place ripple-borrow subtractor - 9, а Parallel Carry-lookahead схема має близьке значення 10, але при цьому демонструє кращу паралелізацію за CNOT-depth.

Kogge–Stone subtractor має найбільшу кількість кубітів і гейтів на абстрактному рівні. Це пов'язано з тим, що parallel-prefix структура вимагає додаткових проміжних регістрів і більшої кількості Toffoli-подібних операцій. Для n=3 переваги логарифмічної глибини ще не проявляються, тому накладні витрати домінують. На рис. 1-6 представлені квантові схеми відповідних віднімачів.

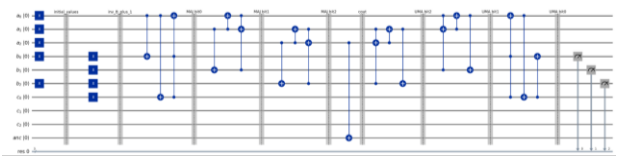

Рис. 1. Схема Cuccaro ripple-carry substractor

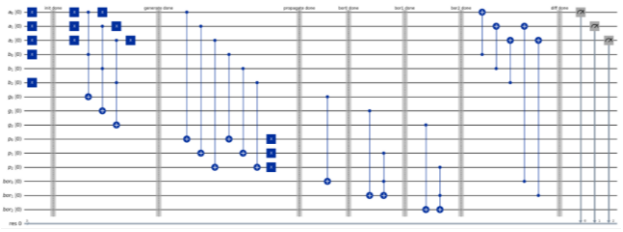

Рис. 2. Parallel Carry-lookahead substractor

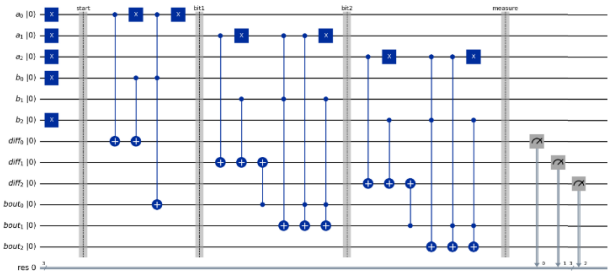

Рис. 3. Out-of-place ripple-borrow substractor

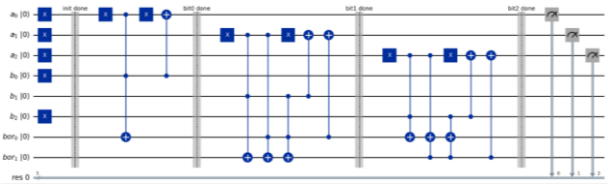

Рис. 4. In-place ripple-borrow substractor

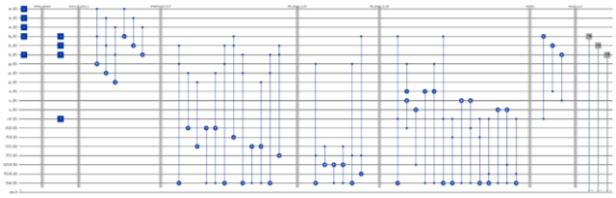

Рис. 5. Kogge–Stone parallel substractor

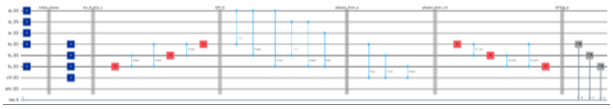

Рис. 6. QFT-based Draper substractor

4.2. Рівень після транспіляції. Після транспіляції найкращі показники серед Clifford+T-орієнтованих схем має Parallel Carry-lookahead subtractor. Він має найменшу загальну кількість гейтів серед транспільованих схем без урахування QFT-аномалії, найменшу глибину, найменший CNOT-depth, найменший T-count і найменший T-depth. Це свідчить, що навіть для малого n=3 паралельне обчислення сигналів позики може бути вигідним.

Cuccaro ripple-carry subtractor має помірну кількість кубітів і прийнятний T-count, але його глибина 76 перевищує глибину carry-lookahead схеми більш ніж удвічі. Out-of-place ripple-borrow має найменшу абстрактну глибину, однак після декомпозиції Toffoli-гейтів поступається carry-lookahead за T-depth і CNOT-depth. In-place ripple-borrow економить кубіти, але ця економія досягається ціною більшої послідовності операцій.

Kogge–Stone subtractor виявився найдорожчим серед не-QFT схем: 381 гейт, 162 CNOT і T-count 168. Для трирозрядного випадку така схема є надмірною, оскільки overhead parallel-prefix мережі перевищує виграш від паралелізму. Однак для більших n ця архітектура може стати конкурентнішою завдяки кращому асимптотичному масштабуванню глибини, що відповідає ідеї класичного Kogge–Stone додавання [8].

Таблиця 2

Значення метрик після транспіляції

№	Схема	Гейтів	Depth	CNOT-count	CNOT-depth	T-count	T-depth
1	Cuccaro ripple-carry	112	76	49	45	42 (T=24, $T^{\dagger}$=18)	30
2	Parallel Carry-lookahead	103	33	44	21	35 (T=20, $T^{\dagger}$=15)	15
3	Out-of-place ripple-borrow	116	53	50	32	49 (T=28, $T^{\dagger}$=21)	25
4	In-place ripple-borrow	113	63	47	39	49 (T=28, $T^{\dagger}$=21)	30
5	Kogge–Stone	384	214	162	128	168 (T=96, $T^{\dagger}$=72)	106
6	QFT-based Draper	304881	214256	30	28	167612 (T=83810, $T^{\dagger}$=803802	128087

QFT-based Draper subtractor має лише 30 CNOT-гейтів, що є найкращим показником серед усіх схем після транспіляції. Проте загальна кількість гейтів, T-count і T-depth є надзвичайно великими: 304881 гейт, T-count 167612 і T-depth 128087. Це пояснюється тим, що контрольовані фазові зсуви CP, природні для QFT-арифметики, розкладаються у заданий дискретний Clifford+T-базис із дуже високою вартістю. Отже, QFT-based subtractor не слід оцінювати лише за CNOT-count; для fault-tolerant реалізації ключовими стають T-метрики. Головною перевагою цієї схеми є те, що на абстрактному рівні вона використовує переважно гейти Hadamard- та контрольовані фазові операції CP і має малу кількість CNOT після транспіляції. Тому така схема може бути вигідною на NISQ-пристроях або спеціалізованих архітектурах (trapped-ion платформах), де фазові повороти та контрольовані фазові гейти реалізуються нативно, з малою похибкою і без дорогого розкладу в Clifford+T. У такій моделі вартості важливішими стають кількість двокубітних операцій, зв'язність між кубітами та фізична тривалість гейтів, а не лише T-count.

Таким чином, QFT-based Draper subtractor демонструє конкурентні показники на абстрактному рівні і є привабливим для платформ із підтримкою фазових обертань з використанням гейтів CP або у контексті алгоритмів, що вже оперують у Фур'є-базисі. Однак у fault-tolerant архітектурі з Clifford+T-базисом транспіляція контрольованих фазових обертань спричиняє вибухове зростання T-count і T-depth, що робить цю архітектуру непрактичною для даного контексту.

Отже, вибір схеми віднімача суттєво залежить від цільової апаратної платформи та обчислювальної моделі.

Отримані результати демонструють, що порівняння квантових віднімачів суттєво залежить від обраного рівня абстракції. На логічному рівні QFT-based схема виглядає компактною, оскільки містить лише 15 контрольованих фазових гейтів, 6 Hadamard-гейтів і 9 X-гейтів. Однак після приведення до Clifford+T-базису її вартість різко зростає. Це узгоджується з відомими властивостями QFT-арифметики: вона ефективна за наявності нативних або наближено реалізованих фазових обертань, але може бути невигідною в дискретних fault-tolerant базисах [10, 11].

Для схем на основі Toffoli-логіки основним джерелом вартості є розкладання CCX у Clifford+T-базис. Саме тому T-count корелює з кількістю Toffoli-гейтів на абстрактному рівні. Наприклад, Kogge-Stone схема містить 24 CCX, що після транспіляції призводить до T-count=168. Натомість Parallel Carry-lookahead схема має лише 5 CCX, тому її T-count дорівнює 35.

Важливо також розрізняти in-place та out-of-place реалізації. In-place subtractor використовує менше кубітів, що є перевагою для пристроїв із обмеженою кількістю фізичних або логічних кубітів. Проте така схема зазвичай має складнішу послідовність операцій, оскільки результат записується поверх одного з вхідних регістрів. Out-of-place підхід потребує окремого регістра результату, але може мати простішу структуру обчислення різниці та позики.

Parallel Carry-lookahead subtractor у цьому експерименті є найкращим компромісом між глибиною та T-вартістю. Він використовує більше кубітів, ніж ripple-borrow схеми, але виграє за критичними метриками після транспіляції. Для fault-tolerant квантових обчислень це особливо важливо, оскільки зменшення T-depth безпосередньо впливає на час виконання логічної схеми [9].

Cuccaro ripple-carry subtractor залишається важливим baseline-рішенням. Його цінність полягає у простоті, регулярності та добре вивченій структурі [6]. Такі схеми є зручними для перевірки коректності, побудови більших арифметичних блоків і порівняння з оптимізованими архітектурами.

5. Висновки. У роботі виконано порівняльний аналіз шести квантових схем віднімання для трирозрядних операндів у Qiskit. Після транспіляції до базису {CX, T, $T^{\dagger}$, H, X, S, $S^{\dagger}$} найефективнішою серед розглянутих Clifford+T-орієнтованих схем виявилася Parallel carry-lookahead схема: вона має 102 гейти, глибину 33, CNOT-depth 21, T-count 35 і T-depth 15.

In-place ripple-borrow subtractor є найекономнішою схемою за кількістю кубітів серед Toffoli-базованих реалізацій, але поступається carry-lookahead за глибиною та T-depth. Out-of-place ripple-borrow має просту структуру та малу абстрактну глибину, однак після транспіляції не є найкращим за T-метриками. Cuccaro ripple-carry subtractor є корисним baseline, але для заданих параметрів програє carry-lookahead за глибиною. Kogge-Stone subtractor для n = 3 має надмірні накладні витрати, хоча його parallel-prefix природа може бути перспективною для більших розрядностей.

QFT-based Draper subtractor демонструє принципово інший профіль: мала кількість CNOT-гейтів, але надзвичайно велика Clifford+T-вартість через декомпозицію контрольованих фазових обертань. Тому для справедливого оцінювання QFT-based арифметики потрібно або використовувати нативний фазовий базис, або явно задавати точність апроксимації фазових гейтів.

З навчально-методичного погляду проведений аналіз має цінність як приклад переходу від абстрактного опису квантового алгоритму до його схемної та ресурсної реалізації. Порівняння різних квантових схем віднімачів дає змогу студентам побачити, що одна й та сама арифметична операція може реалізовуватися за різними архітектурними принципами: через фазові зсуви, послідовне поширення позики, паралельне обчислення переносів або допоміжні регістри. Такий аналіз формує розуміння того, що вибір квантового алгоритму або схеми не є універсальним, а залежить від цільової архітектури, доступного набору гейтів, кількості кубітів, обмежень на глибину схеми та вартості fault-tolerant реалізації. Отже, розгляд квантових віднімачів може бути використаний в освітньому процесі як практичний інструмент для засвоєння зв'язку між теоретичною моделлю квантових обчислень, логічною схемою та її фізичною реалізацією.

Література

1. Feynman, R. P. Simulating Physics with Computers. *International Journal of Theoretical Physics*. 1982. Vol. 21. P. 467–488. DOI: https://doi.org/10.1007/bf02650179

2. Nielsen, M. A., Chuang, I. L. *Quantum Computation and Quantum Information*. 10th Anniversary ed. Cambridge: Cambridge University Press, 2010. 702 p.

3. Wong, T. G. *Introduction to Classical and Quantum Computing*. Omaha, NE: Rooted Grove, 2022. 400 p.

4. Preskill, J. *Course Information for Physics 219/Computer Science 219: Quantum Computation*. California Institute of Technology, 2015–2025. URL: https://www.preskill.caltech.edu/ph219/

5. Vedral, V., Barenco, A., Ekert, A. Quantum networks for elementary arithmetic operations. *Physical Review A*. 1996. Vol. 54, No. 1. P. 147–153. DOI: https://doi.org/10.1103/PhysRevA.54.147

6. Cuccaro, S. A., Draper, T. G., Kutin, S. A., Moulton, D. P. A new quantum ripple-carry addition circuit. arXiv:quant-ph/0410184, 2004. URL: https://arxiv.org/abs/quant-ph/0410184

7. Draper, T. G., Kutin, S. A., Rains, E. M., Svore, K. M. A logarithmic-depth quantum carry-lookahead adder. *Quantum Information and Computation*. 2006. Vol. 6, No. 4–5. P. 351–369. DOI: https://doi.org/10.26421/QIC6.4-5-4

8. Kogge, P. M., Stone, H. S. A parallel algorithm for the efficient solution of a general class of recurrence equations. *IEEE Transactions on Computers*. 1973. Vol. C-22, No. 8. P. 786–793. DOI: https://doi.org/10.1109/TC.1973.5009159

9. Gidney, C. Halving the cost of quantum addition. *Quantum*. 2018. Vol. 2. Article 74. DOI: https://doi.org/10.22331/q-2018-06-18-74

10. Ruiz-Perez, L., Garcia-Escartin, J. C. Quantum arithmetic with the Quantum Fourier Transform. *Quantum Information Processing*. 2017. Vol. 16. Article 152. DOI: https://doi.org/10.1007/s11128-017-1603-1

11. Draper, T. G. Addition on a Quantum Computer. arXiv:quant-ph/0008033, 2000. URL: https://arxiv.org/abs/quant-ph/0008033

12. Mykhailova, M. *Quantum Programming in Depth: Solving Problems with Q# and Qiskit*. Manning Publications, 2025.

13. Norlén, H. *Quantum Computing in Practice with Qiskit® and IBM Quantum Experience®*. Birmingham: Packt Publishing, 2020. 354 p.

14. Loredo, J. *Learn Quantum Computing with Qiskit*. 2nd ed. Birmingham: Packt Publishing, 2024. 582 p.

Polupan Yu.V. Comparative analysis of quantum subtraction circuits in the basis of modern quantum processors.

The paper investigates six quantum subtraction circuits implemented in the Qiskit framework: the out-of-place ripple-borrow subtractor, in-place ripple-borrow subtractor, Cuccaro ripple-carry subtractor, parallel carry-lookahead subtractor, parallel-prefix Kogge–Stone subtractor, and the QFT-based subtractor following Draper's approach. The aim of the study is to compare these circuits in terms of qubit count, gate count, circuit depth, CNOT count, CNOT depth, T-count, and T-depth after transpilation to the {CX, T, T†, H, X, S, S†} basis. It is shown that for three-bit operands, the in-place ripple-borrow and QFT-based circuits require the fewest qubits, while the Parallel Carry-lookahead subtractor demonstrates the smallest transpiled depth. The QFT-based circuit has a low number of CNOT gates; however, after decomposing controlled phase rotations (CP) into the Clifford+T basis, its T-cost becomes several orders of magnitude higher than that of the other circuits. The obtained results confirm that the choice of subtractor architecture depends on the target computational model: for fault-tolerant Clifford+T implementations, circuits with controlled T-complexity are preferable, whereas the QFT approach is more appropriate to evaluate in native phase bases.

Overall, the results show that for small bit-widths and Clifford+T-oriented implementations, the most

balanced choice is the Parallel Carry-lookahead subtractor, while ripple-borrow circuits remain attractive under qubit-limited conditions. The QFT-based approach requires separate analysis in hardware models where phase shifts are cheaper or natively supported.

From a teaching and methodological perspective, such an analysis is important for developing students' practical understanding of the architectural diversity of quantum arithmetic circuits. Comparing different types of subtractors demonstrates that the same operation can be implemented using fundamentally different approaches, which manifest differently at both logical and physical levels. This enables students to realize that the choice of an algorithm or circuit implementation depends not only on the mathematical formulation of the problem, but also on the target quantum architecture, the native gate set, the number of available qubits, and the requirements for fault-tolerant execution.

Keywords: *quantum computing, quantum arithmetic, quantum subtraction, subtractor, Qiskit, Clifford+T, ripple-borrow, carry-lookahead, Kogge–Stone, QFT, Draper adder.*

Полупан Юлія Вікторівна – к.т.н., доц., кафедра Інформатики та програмної інженерії, КПІ ім. І. Сікорського, м. Київ,
https://orcid.org/0009-0000-0243-824X
e-mail: Juliy_polupan@i.ua

Дата першого надходження статті 15.02.2026.
Дата прийняття статті до друку після рецензування 25.03.2025.
Дата публікації 11.05.2026.