Quantum Information and Computation, Vol. 23, No. 13&14 (2023) 1081–1090

IMPLEMENTING THE QUANTUM FANOUT OPERATION WITH SIMPLE PAIRWISE INTERACTIONS[a]

STEPHEN FENNER
Computer Science and Engineering Department, University of South Carolina
Columbia, South Carolina 29208 USA

RABINS WOSTI
Computer Science and Engineering Department, University of South Carolina
Columbia, South Carolina 29208 USA

Received July 5, 2023
Revised October 10, 2023

It has been shown that, for even n, evolving n qubits according to a Hamiltonian that is the sum of pairwise interactions between the particles, can be used to exactly implement an $(n+1)$-qubit fanout gate using a particular constant-depth circuit [arXiv:quant-ph/0309163]. However, the coupling coefficients in the Hamiltonian considered in that paper are assumed to be all equal. In this paper, we generalize these results and show that for all n, including odd n, one can exactly implement an $(n+1)$-qubit parity gate and hence, equivalently in constant depth an $(n+1)$-qubit fanout gate, using a similar Hamiltonian but with unequal couplings, and we give an exact characterization of the constraints that the couplings must satisfy in order for them to be adequate to implement fanout via the same circuit.

In particular, we show the following: Letting J_{ij} be the coupling strength between the i^{th} and j^{th} qubits, the set of couplings $\{J_{ij}\}$ is adequate to implement fanout via the circuit above if and only if there exists $J > 0$ such that

1. each J_{ij} is an odd integer multiple of J, and
2. for each i, there are an even number of $j \neq i$ such that $J_{ij}/J \equiv 3 \pmod 4$.

Keywords: constant-depth quantum circuit; quantum fanout gate; Hamiltonian; pairwise interactions; spin-exchange interaction; Heisenberg interaction; modular arithmetic

1 Introduction

1.1 Previous work

In the study of classical Boolean circuit complexity, the fanout operation—where a Boolean value on a single wire is copied into any number of wires—is taken for granted as cost-free. The picture is very different, however, with quantum circuits with unitary gates, where the number of wires is fixed throughout the circuit. There, fanout gates are known to be very powerful primitives for making shallow quantum circuits [1–4]. It has been shown that in the quantum realm, fanout, parity (see below), and Mod_q gates (for any $q \geq 2$) are all equivalent up to constant depth and polynomial size [1, 3]. That is, each gate above can be simulated exactly by a constant-depth, polynomial-size quantum circuit using any of the

[a]This is the journal version of arxiv:2203.01141 through Section 4.

other gates above, together with standard one- and two-qubit gates (e.g., C-NOT, H, and T). This is not true in the classical case, where, for example, parity cannot be computed by constant-depth, polynomial-size Boolean circuits with fanout and unbounded AND-, OR-, and NOT-gates [5–7]. Furthermore, using fanout gates, in constant depth and polynomial size one can approximate sorting, arithmetical operations, phase estimation, and the quantum Fourier transform [2, 4]. Fanout gates can also exactly implement n-qubit threshold gates, unbounded AND-gates (generalized Toffoli gates), and OR-gates in constant depth [8]. Since long quantum computations may be difficult to maintain due to decoherence, shallow quantum circuits may prove much more realistic, at least in the short term, and finding ways to implement fanout would then lend enormous power to these circuits.

On the negative side, fanout gates so far appear hard to implement by traditional quantum circuits. There is mounting theoretical evidence that fanout gates cannot be simulated in small (sublogarithmic[b]) depth and small width, even if unbounded AND-gates are allowed [9, 10].

Therefore, rather than trying to implement fanout with a traditional small-depth quantum circuit, an alternate approach would be to evolve an n-qubit system according to one or more (hopefully implementable) Hamiltonians, along with a minimal number of traditional quantum gates. It was shown in [11, 12] that simple Hamiltonians using spin-exchange (Heisenberg) interactions do exactly this. Those papers presented a simple quantum circuit for computing n-bit parity (equivalent to fanout) that included two invocations of the Hamiltonian along with a constant number of one- and two-qubit Clifford gates.

More recently, Guo et al. [13] presented a method for implementing fanout on a mesh of qubits. Their approach involves a series of modulated long-range Hamiltonians applied to the qubits obeying inverse power laws.

1.2 The current work

This paper revisits the spin-exchange Hamiltonians considered in [11, 12]. A major weakness of that work is that it assumes all the pairwise couplings between the spins to be equal. This is physically unrealistic since we expect couplings between spins that are spatially far apart to be weaker than those between spins in close proximity.

In this paper, we show that n-qubit fanout can still be implemented by the exact same circuit C_n given in [12], even with a wide variety of unequal pairwise couplings. We show that the couplings must satisfy certain constraints in order for C_n to implement fanout.

Formally, the n-qubit fanout gate F_n and the n-qubit parity gate P_n are $(n + 1)$-qubit unitary operators defined such that

$$F_n \left| x_1, \ldots, x_n, c \right\rangle = \left| x_1 \oplus c, \ldots, x_n \oplus c, c \right\rangle \ ,$$
$$P_n \left| x_1, \ldots, x_n, t \right\rangle = \left| x_1, \ldots, x_n, t \oplus x_1 \oplus \cdots \oplus x_n \right\rangle \ ,$$

for all $x_1, \ldots, x_n, c, t \in \{0, 1\}$. It was shown in [3] that $F_n = H^{\otimes(n+1)} P_n H^{\otimes(n+1)}$, where H is the 1-qubit Hadamard gate. Thus F_n and P_n are equivalent in constant depth, and any circuit implementing P_n can be converted to one implementing F_n by conjugating with a bank of Hadamard gates.

The circuit C_n given in [12] implements P_n and is shown in Figure 1. Here, the 1-qubit Clifford gate G_n is either S, I, $S^\dagger$, or Z, depending on $n \bmod 4$, where I is the identity, S

[b]Fanout on n qubits can be implemented by a $O(\log n)$-depth circuit with $O(n)$ many C-NOT gates.

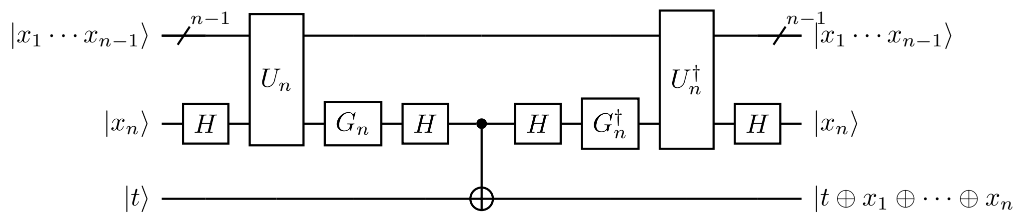


Fig. 1. The circuit C_n implements the parity gate P_n. It uses the unitary operator U_n and its adjoint once each. Here, $G_n = S^{1-n}$ is either S (the phase gate), I, $S^\dagger$, or Z (the Pauli z-gate) if n is congruent to 0, 1, 2, or 3, respectively, mod 4. Since U_n is swap-invariant, the single-qubit gates can be moved to any of the first n qubits, together with the control of the C-NOT gate.

satisfies $S|b\rangle = i^b|b\rangle$ for $b \in \{0,1\}$, and Z is the Pauli z-gate. The unitary operator U_n is defined as follows: for all $x = x_1 \cdots x_n \in \{0,1\}^n$, letting $w = x_1 + \cdots + x_n$,

$$U_n|x\rangle = i^{w(n-w)}|x\rangle \ . \tag{1}$$

It was shown in [12] that U_n is the result of running a particular Hamiltonian H_n, defined below, for a certain amount of time on the first n qubits. It also was shown that $C_n = P_n$ for even n, and a similar calculation shows the same is true for odd n. For the full result and its proof, see Appendix A.

We consider Hamiltonians of the form $H_n = \sum_{1\le i<j\le n} J_{i,j} Z_i Z_j$, where Z_i and Z_j are Pauli Z-gates acting on the i^{th} and j^{th} qubits, respectively, and the $J_{i,j}$ are real coupling constants (in units of energy). H_n is a simplified version of the spin-exchange interaction, where only the z-components of the spins are coupled. It bears some resemblance to a quantum version of the Ising model, as described in [14], but with no transverse field and allowing long-range as well as nearest-neighbor couplings. In [12] it was shown that $U_n = e^{-iH_n t}$ for a certain time t, provided all the coupling constants $J_{i,j}$ are equal.

In this paper, we characterize when H_n can be run to implement U_n by proving the following result in Section 3:

Theorem 1.1 *$U_n \propto e^{-iH_n t}$ for some $t > 0$ if and only if there exists a constant $J > 0$ such that (1.) all $J_{i,j}$ are odd integer multiples of J, and (2.) the graph G on vertices $1, \ldots, n$ with edge set $\{\{i,j\} : i < j$ and $J_{i,j}/J \equiv 3 \pmod 4\}$ is Eulerian[c]; that is, all its vertices have even degree.*

Furthermore, if t exists, we can set $t := \pi\hbar/4J$.

Our result gives more flexibility in the coupling constants, allowing stronger and weaker couplings for spins placed nearer and farther apart, respectively. For example, suppose we have four identical spins arranged in the corners of a square. The spins diagonally opposite each other may have coupling constant J whereas neighboring spins can have coupling constant $3J$. The corresponding couplings are thus congruent to $3 \pmod 4$ for neighboring spins, but this arrangement can be used to implement U_4, because the edges connecting neighboring spins form a square, which is Eulerian. For the spins arranged in the corners of a regular cube, neighboring spins may have coupling constant $7J$, spins on the diagonal ends of each face may have coupling constant $3J$, and the antipodal spins may have coupling constant J. Thus, the corresponding graph G has edges between the neighboring and diagonal spins, and

[c]We use this term in the looser sense that the graph need not be connected.

therefore this arrangement can be used to implement U_8 because the edges connecting the neighboring spins and the spins on the diagonal ends of each face of a regular cube form an Eulerian graph (each vertex has degree 6). Similarly, for spins arranged on the corners of a regular octahedron, the graph of neighboring spins is Eulerian, so neighboring spins can have coupling $3J$ and antipodal spins J.

Our work differs from the recent work of Guo et al. [13] in a number of respects. They adapt a state transfer protocol of Eldredge et al. [15] that, given an arbitrary 1-qubit state $\alpha|0\rangle + \beta|1\rangle$, produces the GHZ-like state $\alpha|0\cdots0\rangle + \beta|1\cdots1\rangle$ on n qubits. Their protocol uses long-range interactions on a mesh of qubits by sequentially turning on and off various Hamiltonians to implement a cascade of C-NOT gates, where different Hamiltonians must be applied at different times. Our scheme runs a simple, swap-invariant Hamiltonian twice, together with a constant number of 1-qubit gates and a C-NOT gate connecting to the target. Unlike in [13], our scheme needs no ancilla qubits.

2 Preliminaries

We use ":=" to mean "equals by definition." We choose physical units so that $\hbar = 1$. We let $\mathbb{Z}$ denote the set of integers. For nonnegative $n \in \mathbb{Z}$, we set $[n] := \{1, \ldots, n\}$; for bit vector $x \in \{0,1\}^n$, we let $w(x)$ denote the Hamming weight of x, and we let x_i denote the i^{th} bit of x, for $1 \leq i \leq n$. For $x, y, \alpha \in \mathbb{R}$ with $\alpha > 0$, we write $x \equiv_\alpha y$ to mean that $(x-y)/\alpha$ is an integer, and we let $x \bmod \alpha$ denote the unique $y \in [0, \alpha)$ such that $x \equiv_\alpha y$. For bits $a, b \in \{0,1\}$ we write $a \oplus b$ to mean $(a+b) \bmod 2$. For vectors or operators U and V of the same type, we write $U \propto V$ to mean there exists $\theta \in \mathbb{R}$ such that $U = e^{i\theta}V$, i.e., U and V differ by a global phase factor.

3 Main Results

We consider a particular type of Hamiltonian H_n, acting on a system of $n \geq 1$ qubits, as the weighted sum of pairwise Z-interactions among the qubits in analogy to spin-exchange (Heisenberg) interactions:

$$H_n := \sum_{1 \leq i < j \leq n} J_{i,j} Z_i Z_j \;, \tag{2}$$

where Z_k is the Pauli Z-gate acting on the k^{th} qubit for $k \in [n]$, and for $1 \leq i < j \leq n$, $J_{i,j} \in \mathbb{R}$ is the coupling coefficient between the i^{th} and j^{th} qubits. For convenience, we define $J_{j,i} := J_{i,j}$ for all $1 \leq i < j \leq n$. H_n differs from the usual (isotropic) Heisenberg interactions in that only the z-components of the spins are coupled.

Let $x = x_1 \cdots x_n \in \{0,1\}^n$ be a vector of n bits. Notice that $Z_i Z_j |x\rangle = (-1)^{x_i + x_j} |x\rangle$ for $1 \leq i < j \leq n$, that is, $Z_i Z_j$ flips the sign of $|x\rangle$ iff $x_i \neq x_j$. Further, for $t, \theta \in \mathbb{R}$, let

$$V_n := V_n(t, \theta) := e^{-i\theta} e^{-iH_n t} \tag{3}$$

be the unitary operator realized by evolving the Hamiltonian H_n of Eq. (2) for time period t, where θ represents a global phase factor that may be introduced into the system. It has been explicitly shown in [12] that for $n \equiv_4 2$, if $V_n \propto U_n$ (see Eq. (1)), one can realize the parity gate P_n (and thus the fanout gate F_n) in constant additional depth for n qubits via the quantum circuit C_n shown in Figure 1. This fact indeed holds for all n via the same circuit, and we give a unified proof of this in Appendix A. Further, it was shown in the same paper that $V_n \propto U_n$ if all the $J_{i,j}$ are equal, and we give an updated proof of this in Appendix B, where we prove the following:

Lemma 3.1 *For $n \geq 1$, let $H_n := J \sum_{1 \leq i < j \leq n} Z_i Z_j$ for some $J > 0$. Then $U_n = V_n(t, \theta)$ for some $\theta \in \mathbb{R}$, where $t := \pi/(4J)$ and $V_n(t, \theta)$ is as in Eq. (3).*[d]

Proof. See Appendix B. □.

The main goal of this paper is to show that equality of the $J_{i,j}$ is not necessary in order to realize the unitary operator U_n. In fact, we give an exact characterization of the values of the couplings $J_{i,j}$ that make this possible (Theorem 1.1). We will use Lemma 3.1 to establish Theorem 1.1, whose proof is at the end of this section.

Let H_n be as in Eq. (2) for arbitrary $J_{i,j}$. For $x \in \{0,1\}^n$ and $t, \theta_1 \in \mathbb{R}$, setting $k_{i,j} := J_{i,j} t$ for convenience, we have

$$V_n(t, \theta_1) |x\rangle = \exp\left(-i\theta_1 - i \sum_{1 \leq i < j \leq n} k_{i,j} (-1)^{x_i + x_j} \right) |x\rangle \ . \tag{4}$$

Using the fact that $U_n |x\rangle = \exp(i(\pi/2) w(x)(n - w(x))) |x\rangle$ and equating exponents, the condition that $V_n(t, \theta_1) = U_n$ is seen to be equivalent to

$$\theta_1 + \sum_{1 \leq i < j \leq n} k_{i,j} (-1)^{x_i + x_j} \equiv_{2\pi} -\left(\frac{\pi}{2}\right) w(x)(n - w(x)) \tag{5}$$

holding for all $x = x_1 \cdots x_n \in \{0,1\}^n$. Lemma 3.1 yields a similar phase congruence in the case where $k_{i,j} = Jt = \pi/4$ for all $i < j$: there exists $\theta_2 \in \mathbb{R}$ such that for all $x \in \{0,1\}^n$,

$$\theta_2 + \frac{\pi}{4} \sum_{1 \leq i < j \leq n} (-1)^{x_i + x_j} \equiv_{2\pi} -\left(\frac{\pi}{2}\right) w(x)(n - w(x)) \ . \tag{6}$$

Subtracting Eq. (6) from Eq. (5) and rearranging, we get that $V_n(t, \theta) = U_n$ is equivalent to

$$\sum_{1 \leq i < j \leq n} \left(k_{i,j} - \frac{\pi}{4}\right) (-1)^{x_i + x_j} \equiv_{2\pi} \theta_2 - \theta_1 \qquad \forall x \in \{0,1\}^n \ ,$$

or equivalently, setting $f_{i,j} := k_{i,j} - \pi/4$ for all $1 \leq i < j \leq n$,

$$\sum_{1 \leq i < j \leq n} f_{i,j} (-1)^{x_i + x_j} \equiv_{2\pi} \theta_2 - \theta_1 \qquad \forall x \in \{0,1\}^n \ . \tag{7}$$

Substituting the zero vector for x in Eq. (7) implies $\theta_2 - \theta_1 \equiv_{2\pi} \sum_{i<j} f_{i,j}$, so Eq. (7) can be rewritten as

$$\begin{aligned} \sum_{i<j} f_{i,j} (-1)^{x_i + x_j} &\equiv_{2\pi} \sum_{i<j} f_{i,j} \\ \sum_{i<j} f_{i,j} \left((-1)^{x_i + x_j} - 1\right) &\equiv_{2\pi} 0 \\ \sum_{i<j \,:\, x_i \neq x_j} f_{i,j} &\equiv_{\pi} 0 \qquad \forall x \in \{0,1\}^n \ . \end{aligned} \tag{8}$$

[d] J is in units of energy and t is in units of time, but this fact is irrelevant to our results; one can assume that J and t are unitless quantities. In any case, Jt is unitless, as we are taking $\hbar := 1$.

(The line above includes an implicit division by -2.) We have thus established the following lemma:

Lemma 3.2 *Let H_n be as in (2) and let $t \in \mathbb{R}$ be arbitrary. There exists $\theta \in \mathbb{R}$ such that $V_n(t,\theta) = U_n$, if and only if Eq. (8) holds, where $f_{i,j} := J_{i,j}t - \pi/4$ for all $1 \le i < j \le n$.*

Lemma 3.3 *Let $\{f_{i,j}\}_{1\le i<j\le n}$ be real numbers such that Eq. (8) holds. Then $f_{i,j} \equiv_{\pi/2} 0$ for all $1 \le i < j \le n$.*

Proof. For convenience, define $f_{j,i} := f_{i,j}$ for all $i < j$. For $a \in [n]$, let $x^{(a)} \in \{0,1\}^n$ be the n-bit vector whose a^{th} bit is 1 and whose other bits are all 0. Consider two different bit vectors $x^{(a)}$ and $x^{(b)} \in \{0,1\}^n$ for $a < b$. Also, consider a third bit vector $y \in \{0,1\}^n$ with $w(y) = 2$ such that its bits are set to 1 in exactly the a and b positions, i.e., $y = x^{(a)} \oplus x^{(b)}$. Plugging in $x^{(a)}$, $x^{(b)}$, and y, respectively, into Eq. (8), we have

$$\sum_{j\in[n]\,:\,j\neq a} f_{a,j} \equiv_\pi 0 \tag{9}$$

$$\sum_{i\in[n]\,:\,i\neq b} f_{i,b} \equiv_\pi 0 \tag{10}$$

$$\sum_{k\in[n]\,:\,k\notin\{a,b\}} (f_{a,k} + f_{k,b}) \equiv_\pi 0 \tag{11}$$

Eq. (9)+(10)−(11) gives

$$\left(\sum_{j\in[n]\,:\,j\neq a} f_{a,j} - \sum_{k\in[n]\,:\,k\notin\{a,b\}} f_{a,k}\right) + \left(\sum_{i\in[n]\,:\,i\neq b} f_{i,b} - \sum_{k\in[n]:k\notin\{a,b\}} f_{k,b}\right) = 2f_{a,b} \equiv_\pi 0\ . \tag{12}$$

Therefore, $f_{a,b} \equiv_{\pi/2} 0$. Since, a and b are chosen arbitrarily, the conclusion follows. $\square$.

Definition 3.4 *For $n \ge 2$, let M_n be the $2^n \times \binom{n}{2}$ matrix over the 2-element field $\mathbb{F}_2$ with rows m_x indexed by bit vectors x of length n and columns indexed by pairs $\{i,j\}$ for $1 \le i < j \le n$, whose $(x,\{i,j\})^{th}$ entry is $m_{x,\{i,j\}} = x_i \oplus x_j$.*

Lemma 3.5 *Every matrix M_n defined by Definition 3.4 has rank $n-1$, and its rows are spanned by any set of $n-1$ rows m_x for x with Hamming weight 1.*

Proof. All scalar and vector addition below is over $\mathbb{F}_2$. Let $S := \{x \in \{0,1\}^n : w(x) = 1\}$ be the set of n-bit vectors of Hamming weight 1, and let m_S be the set of rows of M_n indexed by elements of S. For n-bit vectors r and s, we can write the $\{i,j\}^{th}$ component of the sum $m_r + m_s$ as

$$(m_r+m_s)_{\{i,j\}} = m_{r,\{i,j\}} + m_{s,\{i,j\}} = (r_i+r_j)+(s_i+s_j) = (r_i+s_i)+(r_j+s_j) = m_{r+s,\{i,j\}}\ ,$$

and thus $m_r + m_s = m_{r+s}$. With this observation, we can infer that every row in the matrix M_n can be expressed as the sum of the rows in m_S. In particular, we have

$$\sum_{x\in S} m_x = m_{11\cdots 1} = \vec{0}\ .$$

This causes a linear dependence among the rows of m_S. The sum of any nonempty proper subset of m_S, however, results in a row indexed by an n-bit vector z containing at least one 0 and one 1, and thus m_z cannot be all zeros, which means there is no linear dependence corresponding to any proper subset of S. It follows that every matrix M_n of the above form has rank $n-1$, and any set of $n-1$ rows with indices in S spans all the rows of M_n. $\square$.

Notice that Lemma 3.3 results in the following corollary as an immediate consequence.

Corollary 3.6 *Let $\{f_{i,j}\}_{1\le i<j\le n}$ be as in Lemma 3.3, and define $g_{i,j} := 2f_{i,j}/\pi$ for all $1 \le i < j \le n$. Then $g_{i,j} \in \mathbb{Z}$ for all $i < j$, and Eq. (8) is equivalent to $M_n g \equiv_2 \vec{0}$, where g is the column vector with entries $g_{i,j}$.*

Proof of Theorem 1.1: Let H_n be as in Eq. (2). For $t > 0$, the statement that $U_n \propto e^{-iH_n t}$ is equivalent to the existence of some $\theta \in \mathbb{R}$ such that $V_n(t,\theta) = U_n$, where $V_n(t,\theta)$ is defined by Eq. (3). By Lemma 3.2, this in turn is equivalent to Eq. (8), i.e., $\sum_{i<j\,:\,x_i\ne x_j} f_{i,j} \equiv_\pi 0$ for all n-bit vectors x, where $f_{i,j} := J_{i,j}t - \pi/4$ for all $1 \le i < j \le n$. From Lemma 3.3 and Corollary 3.6, Eq. (8) holds if and only if

(i) $f_{i,j} \equiv_{\pi/2} 0$ (and therefore, letting $g_{i,j} := 2f_{i,j}/\pi$, we have $g_{i,j} \in \mathbb{Z}$) for all $1 \le i < j \le n$, and

(ii) $M_n g \equiv_2 \vec{0}$, where g is the $\binom{n}{2}$-dimensional column vector of $g_{i,j}$'s and M_n is as in Definition 3.4.

Solving for $J_{i,j}$ in terms of $f_{i,j}$ gives

$$J_{i,j} = \frac{f_{i,j} + \pi/4}{t} = (2g_{i,j}+1)\left(\frac{\pi}{4t}\right) = (2g_{i,j}+1)J$$

for all $1 \le i < j \le n$, where we set $J := \pi/(4t) > 0$, whence $t = \pi/(4J)$. Notice that $J_{i,j}/J = 2g_{i,j}+1$ is an odd integer and

$$\frac{J_{i,j}}{J} \equiv_4 \begin{cases} 1 & \text{if } g_{i,j} \equiv_2 0, \\ 3 & \text{if } g_{i,j} \equiv_2 1. \end{cases} \tag{13}$$

Recall (Lemma 3.5) that the rows of the matrix M_n are spanned by the set S of n-bit vectors with Hamming weight 1. It follows that the condition $M_n g \equiv_2 0$ is equivalent to $m_x g \equiv_2 0$ holding for all $x \in S$. Fix any $r \in [n]$ and let $x := x^{(r)} \in S$ be such that $x_r = 1$ and $x_s = 0$ for all $s \ne r$. Then

$$m_x g \equiv_2 \sum_{1\le i<j\le n} (x_i + x_j) g_{i,j} \equiv_2 \sum_{i<r} g_{i,r} + \sum_{r<j} g_{r,j} \equiv_2 \sum_{i<r\,:\,g_{i,r}\equiv_2 1} g_{i,r} + \sum_{r<j\,:\,g_{r,j}\equiv_2 1} g_{r,j}\ . \tag{14}$$

Let G be the graph with vertex set $[n]$ where an edge connects vertices $i < j$ iff $g_{i,j}$ is odd. Then the right-hand side of Eq. (14) is the degree of the vertex r in G. The condition $m_x g \equiv_2 0$ is then equivalent to the degree of r being even. Since, $r \in [n]$ (and hence $x \in S$) was chosen arbitrarily, this applies to all the vertices of G. Finally, from Eq. (13) we have for all $i < j$ that $J_{i,j}/J \equiv_4 3$ if and only if $g_{i,j}$ is odd, and so the theorem follows. $\square$.

Here is an easy restatement of Theorem 1.1 that avoids graph concepts. (Recall that we set $J_{j,i} := J_{i,j}$ for all $i < j$.)

Corollary 3.7 *$U_n \propto e^{-iH_n t}$ for some $t > 0$ if and only if there exists a constant $J > 0$ such that (1.) all $J_{i,j}$ are odd integer multiples of J, and (2.) for every $i \in [n]$,*

$$\prod_{j\,:\,j\ne i} \frac{J_{i,j}}{J} \equiv_4 1\ .$$

Furthermore, if t exists, we can set $t := \pi\hbar/4J$.

Proof. Fix $i \in [n]$. Given that for all $j \neq i$, either $J_{i,j}/J \equiv_4 1$ or $J_{i,j}/J \equiv_4 3$, the product over all such j is congruent to 1 (mod 4) if and only if the latter congruence holds for an even number of such j. This is the stated condition on the graph in Theorem 1.1. $\Box$.

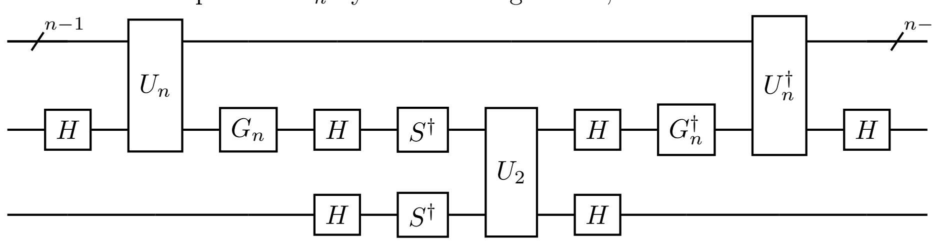
4 Parity Versus U_n

Fix $n \geq 2$. Figure 1 gives a quantum circuit C_n implementing the parity gate P_n using a single U_n gate and its inverse $U_n^\dagger$, together with H-gates, S-gates, and a single C-NOT-gate. In this section we briefly describe some related implementations that tighten this result.

First, we observe that $U_n^4 = I$ for all n, and $U_n^2 = I$ if n is odd. Thus $U_n^\dagger$ can be replaced with U_n^3 or U_n in the circuit C_n, depending on the parity of n. We may also replace the C-NOT gate in C_n with a U_2 gate and some 1-qubit gates: Letting C-Z be the controlled Pauli z-gate, we have

$$\text{C-}Z = (S^\dagger \otimes S^\dagger)U_2 = U_2(S^\dagger \otimes S^\dagger) ,$$

which allows us to implement P_n by the following circuit, which is a modification of C_n:



Thus P_n can be implemented with at most four U_n gates, a single U_2 gate, and constantly many H and S gates.

Conversely, U_n can be implemented with two P_n-gates, a few S-gates, and an ancilla qubit. Let $G := S^{2-n}$, which is Z, S, I, or $S^\dagger$, as n is congruent to 0, 1, 2, or 3 (mod 4), respectively. For any $x \in \{0,1\}^n$, one readily checks that

$$U_n |x\rangle \otimes |0\rangle = (U_n \otimes I)(|x\rangle \otimes |0\rangle) = P_n(G^{\otimes n} \otimes S)P_n(|x\rangle \otimes |0\rangle) ,$$

where I is the 1-qubit identity operator.

5 Conclusions and Further Work

We have concentrated on implementing the operator U_n, which is constant-depth equivalent to fanout. Studying U_n instead of F_n has two theoretical advantages over F_n: (1) U_n is represented in the computational basis by a diagonal matrix; (2) unlike F_n, which has a definite control and targets, U_n is invariant under any permutation of its qubits, or equivalently, it commutes with the SWAP operator applied to any pair of its qubits. Are there other such operators that are both constant-depth equivalent to fanout and implementable by a simple Hamiltonian?

The Hamiltonian H_n only includes the z-components of the spins. In Heisenberg interactions, the x- and y-components should also be included in the Hamiltonian, so that a pairwise coupling between spins i and j would be $J_{i,j}(X_iX_j + Y_iY_j + Z_iZ_j)$. In [11] it was shown that these Hamiltonians can also simulate fanout provided all the pairwise couplings are equal. We believe we can relax the equal coupling restriction for these Hamiltonians as well. One could also ask whether the realization of fanout is possible if one requires that the couplings obey an inverse power law. We will investigate this in a sequel of this paper. (For a preprint, see [16].)

Finally, the time needed to run our Hamiltonian is inversely proportional to the fundamental coupling constant J. If J is small relative to the actual couplings in the system, then this gives a poor time-energy trade-off and will likely be more difficult to implement quickly with precision.

References

[1] F. Green, S. Homer, C. Moore, and C. Pollett, *Counting, fanout and the complexity of quantum ACC*, Quantum Information and Computation **2** (2002), 35–65, available at `quant-ph/0106017`.

[2] P. Høyer and R. Špalek, *Quantum circuits with unbounded fan-out*, Proceedings of the 20th symposium on theoretical aspects of computer science, 2003, pp. 234–246.

[3] C. Moore, *Quantum circuits: Fanout, parity, and counting*, 1999. arXiv:quant-ph/9903046.

[4] R. Špalek, *Quantum circuits with unbounded fan-out*, 2002. arXiv:quant-ph/0208043.

[5] M. Ajtai, Σ_1^1 *formulæ on finite structures*, Annals of Pure and Applied Logic **24** (1983), 1–48.

[6] M. Furst, J. B. Saxe, and M. Sipser, *Parity, circuits, and the polynomial time hierarchy*, Mathematical Systems Theory **17** (1984), 13–27.

[7] J. Håstad, *Computational limitations for small depth circuits*, MIT Press, Cambridge, MA, 1987.

[8] Y. Takahashi and S. Tani, *Collapse of the hierarchy of constant-depth exact quantum circuits*, Computational Complexity **25** (2016), no. 4, 849–881, available at `arXiv:1112.6063`. Conference version in Proceedings of the 28th IEEE Conference on Computational Complexity (CCC 2013).

[9] M. Fang, S. Fenner, F. Green, S. Homer, and Y. Zhang, *Quantum lower bounds for fanout*, Quantum Information and Computation **6** (2006), 46–57, available at `quant-ph/0312208`.

[10] G. Rosenthal, *Bounds on the* QAC^0 *complexity of approximating parity*, 2020. arXiv:2008.07470.

[11] S. Fenner and Y. Zhang, *Implementing fanout, parity, and mod gates via spin exchange interactions*, 2004. arXiv:quant-ph/0407125.

[12] S. A. Fenner, *Implementing the fanout gate by a Hamiltonian*, 2003. arXiv:quant-ph/0309163.

[13] A. Y. Guo, A. Deshpande, S.-K. Chu, Z. Eldredge, P. Bienias, D. Devulapalli, Y. Su, A. M. Childs, and A. V. Gorshkov, *Implementing a fast unbounded quantum fanout gate using power-law interactions*, 2020. arXiv:2007.00662.

[14] Wikipedia, *Transverse-field Ising model*, 2021. `https://en.wikipedia.org/wiki/Transverse-field_Ising_model`.

[15] Zachary Eldredge, Zhe-Xuan Gong, Jeremy T. Young, Ali Hamed Moosavian, Michael Foss-Feig, and Alexey V. Gorshkov, *Fast quantum state transfer and entanglement renormalization using long-range interactions*, Phys. Rev. Lett. **119** (2017Oct), 170503.

[16] S. A. Fenner and R. Wosti, *Implementing the fanout operation with simple pairwise interactions*, 2022. arXiv:2203.01141.

Appendix A The Quantum Circuit for Parity

In this section, we show by direct calculation that the circuit C_n shown in Figure 1 implements the parity gate P_n, for all $n \geq 1$. The special case for $n \equiv 2 \pmod 4$ was shown in [12]. Here, U_n is defined by Eq. (1), and

$$G_n := S^{1-n} = \begin{cases} S & \text{if } n \equiv 0 \pmod 4, \\ I & \text{if } n \equiv 1 \pmod 4, \\ S^\dagger & \text{if } n \equiv 2 \pmod 4, \\ Z & \text{if } n \equiv 3 \pmod 4, \end{cases}$$

where S is the gate satisfying $S|b\rangle = i^b|b\rangle$ for $b \in \{0,1\}$, I is the identity, and Z is the Pauli z-gate. Note that G_n is chosen so that $G_n|b\rangle = i^{b(1-n)}|b\rangle$.

Fix any $x_1,\ldots,x_n,t \in \{0,1\}$. For convenience, we separate the first $n-1$ qubits, which only participate in U_n and $U_n^\dagger$, letting $\vec{x} := x_1 \ldots x_{n-1}$. We set $w := w(\vec{x}) = x_1 + \cdots + x_{n-1}$ and $W := w + x_n$, the Hamming weight of $x_1 \cdots x_n$. We set $p := W \bmod 2$, the parity of $x_1 \cdots x_n$, which will be XORed with t in the target qubit. Running the first half of the circuit starting with initial state $|\vec{x}\rangle|x_n\rangle|t\rangle$, we have

$$\begin{aligned}
|\vec{x}\rangle|x_n\rangle|t\rangle &\xmapsto{H} 2^{-1/2}|\vec{x}\rangle(|0\rangle + (-1)^{x_n}|1\rangle)|t\rangle = 2^{-1/2}(|\vec{x},0\rangle + (-1)^{x_n}|\vec{x},1\rangle)|t\rangle \\
&\xmapsto{U_n} 2^{-1/2}\left(i^{w(n-w)}|\vec{x},0\rangle + (-1)^{x_n} i^{(w+1)(n-w-1)}|\vec{x},1\rangle\right)|t\rangle \\
&= 2^{-1/2} i^{w(n-w)}|\vec{x}\rangle\left(|0\rangle + i^{n-1-2(w+x_n)}|1\rangle\right)|t\rangle \\
&= 2^{-1/2} i^{w(n-w)}|\vec{x}\rangle\left(|0\rangle + (-1)^W i^{n-1}|1\rangle\right)|t\rangle \\
&\xmapsto{G_n} 2^{-1/2} i^{w(n-w)}|\vec{x}\rangle\left(|0\rangle + (-1)^W|1\rangle\right)|t\rangle \\
&= 2^{-1/2} i^{w(n-w)}|\vec{x}\rangle(|0\rangle + (-1)^p|1\rangle)|t\rangle \\
&\xmapsto{H} i^{w(n-w)}|\vec{x}\rangle|p\rangle|t\rangle\ .
\end{aligned}$$

At this point, the C-NOT gate is applied, resulting in the state $i^{w(n-w)}|\vec{x}\rangle|p\rangle|t\oplus p\rangle$. The remaining gates undo the above action on the first n qubits, resulting in the state $|\vec{x}\rangle|x_n\rangle|t\oplus p\rangle$, which is the same as P_n applied to the initial state.

Finally, we note that C_n only depends on U_n up to an overall phase factor: any gate $V_n \propto U_n$ can be substituted for U_n in the circuit, because any phase factor introduced by applying V_n on the left will be cancelled when $V_n^\dagger$ is applied on the right. This fact is, of course, unnecessary for physical implementation.

Appendix B Implementing U_n with Equal Couplings: Proof of Lemma 3.1

In this section, we give an updated proof of Lemma 3.1, which we restate here:

Lemma 5.1 *For $n \geq 1$, let $H_n := J\sum_{1\leq i<j\leq n} Z_iZ_j$ for some $J > 0$. Then $U_n = V_n(t,\theta)$ for some $\theta \in \mathbb{R}$, where $t := \pi/(4J)$ and $V_n(t,\theta)$ is as in Eq. (3).*

Proof. Looking at Eqs. (1) and (3), we see that for $t,\theta \in \mathbb{R}$, the condition $V(t,\theta) = U_n$ is equivalent to

$$\exp\left(-i\theta - i\sum_{1\leq i<j\leq n} Jt(-1)^{x_1+x_j}\right) = i^{w(x)(n-w(x))}$$

holding for all $x \in \{0,1\}^n$. Noting that $i = e^{i\pi/2}$ and $Jt = \pi/4$ and equating exponents, this condition becomes

$$\theta + \frac{\pi}{4}\sum_{1\leq i<j\leq n}(-1)^{x_i+x_j} \equiv_{2\pi} -\left(\frac{\pi}{2}\right)w(x)(n-w(x)) \tag{B.1}$$

for all $x \in \{0,1\}^n$ (cf. Eqs. (4) and (6)). The sum on the left-hand side becomes

$$\begin{aligned}\sum_{i<j}(-1)^{x_i+x_j} &= \frac{1}{2}\sum_{i\neq j}(-1)^{x_i+x_j} = -\frac{n}{2}+\frac{1}{2}\sum_i\sum_j(-1)^{x_i+x_j} = -\frac{n}{2}+\frac{1}{2}\left(\sum_{i=1}^{n}(-1)^{x_i}\right)^2 \\ &= -\frac{n}{2}+\frac{1}{2}\left(\sum_i(1-2x_i)\right)^2 = -\frac{n}{2}+\frac{1}{2}\left(n-2w(x)\right)^2 \\ &= \frac{n^2-n}{2} - 2w(x)(n-w(x))\ .\end{aligned}$$

Substituting this back into Eq. (B.1) satisfies it, provided we set $\theta := -\pi(n^2-n)/8$. $\square$.