Quantum matchgate computations and linear threshold gates

BY MAARTEN VAN DEN NEST*

Max-Planck-Institut für Quantenoptik, Hans-Kopfermann-Straße 1, 85748 Garching, Germany

The theory of matchgates is of interest in various areas in physics and computer science. Matchgates occur, for example, in the study of fermions and spin chains, in the theory of holographic algorithms and in several recent works in quantum computation. In this paper, we completely characterize the class of Boolean functions computable by unitary two-qubit matchgate circuits with some probability of success. We show that this class precisely coincides with that of the linear threshold gates. The latter is a fundamental family that appears in several fields, such as the study of neural networks. Using the above characterization, we further show that the power of matchgate circuits is surprisingly trivial in those cases where the computation is to succeed with high probability. In particular, the only functions that are matchgate-computable with success probability greater than 3/4 are functions depending on only a single bit of the input.

Keywords: matchgates; threshold gates; classical simulations

1. Introduction

One of the great virtues of the field of quantum computation is that it interconnects fundamental questions in physics and computer science. The concept of the quantum computer (Deutsch 1989) precisely captures the intrinsic computational power locked within quantum mechanics (Bernstein & Vazirani 1997), and makes it possible to address deep problems, such as the relationship between quantum and classical computational capabilities (Gottesman 1998; Valiant 2002; Jozsa & Linden 2003). At the same time, within the theory of quantum computation it is possible to characterize, in a precise sense, how ‘hard’ it is to simulate physical systems of interest, such as certain ground state problems (Kitaev et al. 2002) and time evolutions (Lloyd 1996).

Of particular interest, also in recent work, is the class of quantum processes generated by matchgates (Kasteleyn 1961; Temperley & Fisher 1961; DiVincenzo & Terhal 2002; Valiant 2002; Jerrum 2003; Cai & Choudhary 2006a,b; Jozsa & Miyake 2008; Bravyi 2009; Jozsa et al. 2010). The latter is a class of unitary two-qubit operations that are defined by certain algebraic constraints. The theory of matchgates is an instance of a research area that displays strong connections to both physics and computer science (Kasteleyn 1961;
In the study of strongly correlated systems, for example, the dynamics of an important class of one-dimensional quantum systems such as the XY model are modeled by matchgate circuits, i.e. for such Hamiltonians \( H \) one can construct a poly-size matchgate circuit \( C_t \), such that \( C_t = e^{iHt} \), for any time \( t \) (e.g. Jozsa & Miyake 2008). Employing mappings between spin-1/2 systems and fermions, matchgate circuits further describe the dynamics of all non-interacting fermionic systems (DiVincenzo & Terhal 2002). In the theory of quantum computation, matchgates are of particular interest as they provide a key example of the class of non-trivial quantum circuits that cannot offer any speed-up over classical computers (for example, in spite of the complex entangled states such circuits may generate; Valiant 2002; Jozsa & Miyake 2008). In addition, matchgate computations were recently found to be equivalent to space-bounded universal quantum computation (Jozsa et al. 2010). In classical computer science, finally, matchgates occur in various studies related to, for example the theory of holographic algorithms (Valiant 2002; Cai & Choudhary 2006a,b).

The aim of the present paper is to characterize the computational power of matchgate circuits. We will in particular study which Boolean functions\(^1\) can be computed with such circuits. Given an arbitrary matchgate circuit \( U \), the question is asked which Boolean function \( f(x) \) can be computed (probabilistically) by initializing the system in the computational basis state \( |x,0⟩ \) (where \( x \) represents an input string and 0 is a string of ancillary zeros), by subsequently running the circuit \( U \) and finally measuring, say, the first qubit. This setting captures in perhaps the most elementary way the computational power of matchgate circuits, associating with each circuit a yes/no question as commonly done.

We remark that, beyond its natural computer scientific interest, such an investigation is relevant from an intrinsic physical perspective as well. In particular, given the aforementioned equivalences between matchgate circuits, fermionic systems and one-dimensional spin systems, the present work aims at gaining insight into the link between the physics of these systems and their computational capabilities. In this context, one may pose a variety of interesting questions such as: ‘Does the presence of a quantum phase transition in the XY model leave any signature in the associated class of functions, which can be computed by time-evolving such systems’? The present work is also situated within such a programme.

In the following, we will characterize the family of matchgate-computable functions in full generality. We will find that this class precisely coincides with the class of linear threshold gates (LTGs; Dertouzos 1965; Muroga 1971; Siu et al. 1995). The latter is a fundamental family of functions that has been a topic of study since the 1960s and that plays an important role in numerous areas. LTGs occur in the study of neural networks where these functions serve as elementary models of neurons (Rosenblatt 1958; Block 1962; Minsky & Papert 1988) and in circuit complexity theory (Goldmann et al. 1992; Hajnal et al. 1993; Goldmann & Karpinski 1998); cf. Feldman et al. (2006), Sherstov (2008), Kalai et al. (2008).

\(^1\)Henceforth, whenever we refer to a ‘function’ we will often mean a Boolean function. This will be clear from the context.
Khot & Saket (2008), O’Donnell & Servedio (2008), and references within for a number of recent investigations on LTGs. The existence of a connection between matchgates and LTGs may be considered surprising, since \textit{a priori} there is no obvious relation between these two theories.

Below we state the contributions of this work in more precise terms. Here, we highlight some particularly noteworthy aspects of our results.

An interesting phenomenon occurs when considering those functions that are matchgate-computable with \textit{high} success probability. Since a generic matchgate circuit may be a rather complex object, one would expect that this class of functions has some non-trivial character as well. We will show that this intuition is incorrect: any function that is matchgate-computable with success probability greater than $3/4$ is proved to be \textit{trivial} in that any such function can only depend on a \textit{single} bit of the input. The origin of this apparent paradox is the strong set of constraints that are placed on any circuit (matchgate or conventional) that is to compute the correct function value with high probability on \textit{all} inputs. Indeed, a generic circuit does typically \textit{not} fulfil these requirements, and hence does not meaningfully compute any function. The present example thus highlights the significance of bounded-error constraints in a rather striking way: in spite of the potentially complex structure of general matchgate circuits, the only instances which turn out to satisfy the bounded-error constraints are circuits computing mere single-bit—i.e. utterly trivial—functions!

Note that the above feature is of interest from a physics perspective as well: it shows that the non-trivial \textit{physical} properties (such as e.g. the presence of a quantum phase transition) of a family of quantum systems are \textit{not} guaranteed to translate into any non-trivial-associated \textit{computational} model. Indeed, in spite of the interesting physical processes modelled by matchgates, these processes turn out to have trivial power when used as a computer, which is to solve problems with high success probability.

Overall, the results in this paper indicate that matchgate circuits have a rather weak computational power. This is in part reflected in the above phenomenon, but also in an additional result obtained in this work. We will characterize the power of matchgate circuits in terms of a strikingly elementary \textit{classical} computer, which is capable of computing every matchgate-computable function with the same success probability as the optimal matchgate circuit.

\textbf{(a) Related work}

We mention two related investigations. First, in Jozsa \textit{et al.} (2010), the power of matchgate circuits was characterized from a different perspective. It was shown that every $n$-qubit nearest-neighbour matchgate circuit $U$ can be mapped to an equivalent circuit $U'$ of roughly the same size, where $U'$ is composed of \textit{general} unitary gates but acts on a logarithmic number of qubits $n' = O(\log n)$. The reduction from $U$ to $U'$ requires a logarithmic space classical computation. A converse statement, relating arbitrary quantum circuits acting on $m$ qubit lines to matchgate circuits acting on $O(2^m)$ qubits, was also proved. Thus Jozsa \textit{et al.} (2010) characterize the power of matchgate circuits, under log-space classical reductions, as equivalent to space-bounded universal quantum computation. It will be interesting to contrast the study of Jozsa \textit{et al.} (2010) with the present paper in the context of bounded-error matchgate computations; we refer to §6a.
Second, an investigation (Buhrman et al. 2009) similar to the present one was carried out for another important class of classically simulatable quantum circuits viz. the Clifford circuits. It was shown that an $n$-bit Boolean function $f$ is Clifford-computable, if and only if it is an affine function, i.e. $f(x) = a^T x + b$ for some $n$-bit string $a$ and some bit $b$. Moreover, all affine functions are proved to be Clifford-computable with unit success probability.

(b) Notation

In the following, $[n]$ denotes the set of positive integers from 1 to $n$, for any $n$. If $x = (x_1, \ldots, x_n)$ is a string of bits $x_k \in \{0,1\}$, then $\hat{x}$ denotes the $\pm 1$ vector that is obtained by replacing all 0-components of the $n$-bit string $x$ by 1 and all 1-components by $-1$. The symbol $\oplus$ denotes addition modulo 2. The 1-norm of a complex vector $w = (w_1, \ldots, w_n)$ is denoted by $\|w\|_1 := \sum_k |w_k|$.

2. Main results

Here, we summarize the contributions of this paper. To do so, we state some preliminary definitions.

A matchgate$^2$ $G$ is any two-qubit operation with matrix representation

$$G = \begin{bmatrix} a & u & b \\ x & v & y \\ c & d \end{bmatrix}, \quad A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \text{and} \quad B = \begin{bmatrix} u & v \\ x & y \end{bmatrix} \quad (2.1)$$

in the standard basis, where $A$ and $B$ are in $U(2)$ and must have the same determinant. Note that the equal determinant requirement, while seemingly innocent, is an important feature of matchgates. In particular, the theory of classical simulations of matchgate circuits crucially depends on this property; see Jozsa & Miyake (2008) for a discussion. We will consider circuits composed of matchgates acting on nearest-neighbour qubits (assuming a one-dimensional ordering of the qubits), i.e. the standard scenario in which matchgates are considered.

Let $f : \{0,1\}^n \rightarrow \{0,1\}$ be a Boolean function on $n$ bits and let $U$ be an $m$-qubit unitary operation with $m \geq n$. We say that $U$ computes $f$ with probability at least $p$ if for every $n$-bit string $x$, the preparation of the $m$-qubit state $U|x,0\rangle$ (where 0 denotes a string of $m - n$ zeroes) followed by a computational basis measurement of the first qubit$^3$ yields the outcome $f(x)$ with a probability of at least $p$. An $n$-bit Boolean function $f$ is said to be matchgate-computable with probability at least $p$, if there exists a matchgate circuit on $m$ qubits,

$^2$The term ‘matchgate’ sometimes refers to a larger class of operations (tensors), which may be both non-unitary and which may act on more than two qubits, containing the unitary two-qubit gates (2.1) as a subclass; cf. Cai & Choudhary (2006a,b) and Bravyi (2009). In this paper, however, a matchgate is always taken to be a unitary two-qubit operation as defined in equation (2.1).

$^3$For convenience, we always assume that the first qubit is measured. This does not entail any loss of generality when considering matchgates, as any matchgate circuit followed by the measurement of the $k$th qubit line can be mapped to an equivalent matchgate circuit followed by measurement of the first qubit (by an appropriate use of fSWAP gates); see §3.
for some $m \geq n$, which computes $f$ with a probability of at least $p$. Note that in the latter definition neither any restriction is placed on the size of $m$ when compared with $n$, nor on the number of gates in the matchgate circuit compared with $n$. However, below we will find that every matchgate-computable function can be computed by a matchgate circuit acting on at most $n + 1$ qubits (without decreasing the success probability). Moreover, it is known that any matchgate circuit acting on $m$ qubits can be re-expressed as a matchgate circuit of size $O(m^3)$ (see Jozsa & Miyake 2008).

(a) Main theorem

We will show that the class of matchgate-computable functions coincides with the family of LTGs. A Boolean function $f$ on $n$ bits is called an LTG if there exists an $n$-dimensional real vector $w$ and a real constant $\theta$, such that $f(x)$ equals 0 if and only if $w^T \hat{x} + \theta$ is strictly positive. The vector $(w, \theta)$ is called a representation of $f$. Examples of LTGs are the NOT gate, the $n$-bit AND and OR, and the majority gate. We will consider LTGs that are supplemented with a parameter which is called the margin of the LTG. Given an LTG $f$ on $n$ bits with representation $(w, \theta)$, the margin of this representation is defined to be the minimal value of $|w^T \hat{x} + \theta|$ over all $n$-bit strings $x$. The margin $\epsilon$ of $f$ itself is the maximal achievable margin of any representation $(w, \theta)$ of $f$, which is normalized in the sense that $\|w\|_1 + |\theta| = 1$.

The main result of this paper achieves a complete characterization of all matchgate-computable functions:

Theorem 2.1. Let $f$ be a Boolean function on $n$ bits and let $p \in (0.5, 1]$. Then the following statements are equivalent:

(a) $f$ is matchgate-computable with probability at least $p$.

(b) $f$ is an LTG with margin $\epsilon \geq 2p - 1$.

Moreover, (a) holds if and only if there exists a matchgate circuit acting on at most $n + 1$ qubits, which computes $f$ with probability at least $p$.

Note that theorem 2.1 connects the margin $\epsilon$ of an LTG with an optimal success probability $p$ of computing this function using matchgate circuits. In particular, $\epsilon$ is small iff $p$ is small. This implies that the class of LTGs computable with matchgate circuits grows larger as the required probability of success is decreased. When $p$ is allowed to be arbitrarily close to 0.5, the full class of LTGs is matchgate-computable owing to theorem 2.1.

As an immediate corollary of the above result, it follows that matchgate circuits do not have universal classical computational power, even when an unbounded error is allowed, i.e. a success probability strictly greater than 0.5 but (with increasing $n$) potentially exponentially close to 0.5. This property follows immediately from the elementary fact that there exist functions that are not LTGs, such as the two-bit parity gate.

(b) Bounded-error computations

Surprisingly, it follows from theorem 2.1 that matchgate circuits can only compute trivial functions if the computation is to succeed with high probability:
Theorem 2.2. A Boolean function $f$ is matchgate-computable with probability $p > 3/4$ if and only if this function is either constant or depends on a single bit of its input.

Owing to theorem 2.1, any function that is matchgate-computable with probability $p > 3/4$ is an LTG with margin $\epsilon > 1/2$. We will show that the only LTGs having such large margin are constant or depend on one input bit, leading to the proof of theorem 2.2. Note that functions which depend on a single input bit have the very simple form $f(x) = x_k$ or $f(x) = 1 - x_k$ for some $k$, i.e. $f$ returns the $k$th bit of its input or its negation. As discussed in §1, theorem 2.2 is a somewhat unexpected result, given that generic matchgate circuits are rather non-trivial objects, which e.g. describe physical systems that may exhibit an interesting behaviour, such as e.g. quantum phase transitions. In spite of this rich structure, theorem 2.2 shows that the computational power of matchgate circuits is near-vanishing in those cases where the correct answer is to be produced with high probability.

Of particular interest are computations that yield the correct output with a probability that is bounded away from 0.5 by an inverse polynomial in the input size. Let $\mathcal{F} = \{f_n: n = 1, 2, \ldots\}$ be a family of Boolean functions, where $f_n$ acts on $n$ bits and let $\{p_n\}$ be a family of probabilities, where $p_n > 0.5$ and, for $n$ large, $p_n$ is bounded away from 0.5 by an inverse polynomial in $n$. We say that $\mathcal{F}$ is matchgate-computable with poly-bounded error if there exists such a poly-bounded family of probabilities as well as a family of matchgate circuits $\{U_n\}$, such that $U_n$ computes $f_n$ with probability at least $p_n$. It is standard that any computation with poly-bounded error can be promoted to an almost deterministic computation\footnote{That is, the success probability is exponentially (in $n$) close to 1.} by repeating the computation poly($n$) times and taking the majority vote of all the obtained results. Owing to theorem 2.1, the families of Boolean functions that are matchgate-computable with poly-bounded error precisely coincides with those LTGs having poly-bounded margin, i.e. the margin $\epsilon_n$ of $f_n$ scales as an inverse polynomial in $n$. Furthermore, we will show that a family of LTGs has poly-bounded margin if and only if $f_n$ has a representation $(w_n, \theta_n)$, where the coefficients of $w_n$ and $\theta_n$ are integers that are at most polynomially large; such families of threshold gates are said to have polynomial integer weight. This leads to the following concise characterization.

Theorem 2.3. A family of Boolean functions is matchgate-computable with poly-bounded error if and only if it is a family of LTGs with polynomial integer weight.

Remark 2.4. The near-deterministic computation of $n$-bit LTGs with polynomial integer weight is obtained by running the computation poly($n$) times and computing the majority vote of all measurement outcomes. It is intriguing that the majority function is indeed an LTG—and hence matchgate-computable—however, in order to properly amplify the success probability, the majority gate itself needs to be computed with suitably high success probability (the latter e.g. being exponentially close to 1). However, owing to theorem 2.2, the majority function cannot be computed with good success probability by any matchgate circuit. Therefore, to obtain the proper amplification, a final non-matchgate computation is needed to compute the majority vote—even though the latter comes intriguingly close to being suitably matchgate-computable!
As a final result, we will construct a classical computational scheme that is equivalent to the matchgate circuit model in the following sense: any function which is matchgate-computable with probability at least $p$ can be computed with probability at least $p$ with our classical scheme, and vice versa. As we will show, the required classical computer is very simple, as it essentially requires a single sample of a fixed (i.e. independent of the input) probability distribution on the set of integers from 1 to $n+1$, together with the possibility of performing a single bit flip of one of the input bits, depending on the outcome of the sampling. This characterization is a further illustration (in addition to, e.g. theorem 2.2) of the weak computational capabilities of matchgate circuits.

Whereas the general result will be stated below, here we illustrate the scheme with an example. Let $n$ be odd and consider the majority function $f_{\text{maj}}$ on $n$-bits, which is an LTG. It can be shown that the margin of $f_{\text{maj}}$ is $\epsilon_{\text{maj}} = n^{-1}$. Owing to theorem 2.1, the optimal success probability of computing $f_{\text{maj}}$ with a matchgate circuit is

$$p_{\text{maj}} = \frac{\epsilon_{\text{maj}} + 1}{2} = \frac{1}{2} + \frac{1}{2n}. \quad (2.2)$$

Now consider the following elementary classical computation:

— Choose an $n$-bit input string $x$.
— Generate a random integer $k$ between 1 and $n$.
— Output the bit value $x_k$.

It can easily be shown that, for every $x$, the output of this computation is $f_{\text{maj}}(x)$ with probability at least $p_{\text{maj}}$. In other words, the above elementary classical computation is capable of computing the majority function with the same probability of success as the optimal matchgate circuit can!

The above example is not coincidental, as we will show that every LTG $f$ can similarly be associated with a simple classical computation of the above nature.

3. Matchgates

In this section, we recall some basic properties of matchgates, which were defined in equation (2.1). We emphasize that, henceforth, the term ‘matchgate circuit’ will always refer to a circuit composed of matchgates acting on nearest-neighbour qubit lines, as commonly done.

We first recall a celebrated result about the classical simulation of matchgate circuits, first proved in Valiant (2002) and subsequently investigated by a series of other authors (DiVincenzo & Terhal 2002; Cai & Choudhary 2006a,b; Jozsa & Miyake 2008; Bravyi 2009).

**Theorem 3.1.** Consider a poly-size $n$-qubit circuit composed of matchgates acting on nearest-neighbour qubits. The circuit acts on an arbitrary standard basis input and is followed by a standard basis measurement of the first qubit. Let $p_0$ denote the probability of obtaining the bit 0 as an outcome. Then there exists a classical algorithm that computes $p_0$ up to $m$ bits in poly$(n, m)$ time.
As a consequence of this result, there exists a poly-time classical algorithm to sample from (a distribution that is exponentially close to) the distribution \( \{p_0, 1-p_0\} \), i.e. any matchgate computation of the above type can be simulated classically in poly-time.

We discuss some further well-established properties of matchgates, which will be used in the proof of theorem 2.1. We refer to e.g. Jozsa & Miyake (2008) for elementary proofs of these properties.

First, without loss of generality, in the following we will always consider poly-size families of matchgate circuits, as it is known that any, possibly exponential size, \( n \)-qubit matchgate circuit family can be re-expressed as a matchgate circuit family of size \( O(n^3) \). Second, consider the \( n \)-qubit Jordan–Wigner operators:

\[
c_{2k-1} = X_k \prod_{i=1}^{k-1} Z_i \quad \text{and} \quad c_{2k} = Y_k \prod_{i=1}^{k-1} Z_i,
\]

where \( X_k, Y_k \) and \( Z_k \) denote the Pauli \( X \), \( Y \) and \( Z \) operators acting on qubit \( k \), respectively. Then an \( n \)-qubit unitary operation \( U \) is a matchgate circuit (up to a global phase) if and only if there exists an operator \( R \in SO(2n) \) such that, for every \( \mu \in [2n] \), it is the case that

\[
U^\dagger c_\mu U = \sum_{\nu=1}^{2n} R_{\mu\nu} c_\nu.
\]

It further holds that \( U \) is a matchgate circuit if and only if there exists a Hermitian operator \( H \) lying in the linear span of the products \( c_\mu c_\nu \) (where \( \mu \neq \nu \)), such that \( U \propto e^{iH} \). Such an operator \( H \) is sometimes called a quadratic Hamiltonian. Quadratic Hamiltonians describe the physics of systems of non-interacting fermions. We will not discuss this connection to fermionic physics here as it would lead us too far outside of the scope of this work, and we refer to e.g. DiVincenzo & Terhal (2002).

The following are some examples of matchgates and matchgate circuits. The fermionic SWAP (fSWAP) operation is easily seen to be a matchgate. This operation sends the basis state \(|ab\rangle\) to \((-1)^{ab}|ba\rangle\), for every \( a, b = 0, 1 \), i.e. it swaps the qubits and adds an overall minus sign if both qubits are in the state \(|1\rangle\). Other elementary examples of matchgate circuits are the products \( c_\mu c_\nu \) for any \( \mu \neq \nu \). Indeed, any such product can be written as an exponential of a quadratic Hamiltonian. Denoting \( H := i c_\mu c_\nu \) it is easily verified that \( H = H^\dagger = H^2 \). Hence

\[
e^{i\pi/2H} \propto H \propto c_\mu c_\nu,
\]

where in the first identity we have used that \( e^{itH} = (\cos t)I + i(\sin t)H \), since \( H = H^2 \). To obtain a more non-trivial example of a matchgate circuit, consider the Hamiltonian of the one-dimensional transverse Ising model:

\[
H_I = -\sum_{k=1}^{n-1} J_k X_k X_{k+1} - \sum_{k=1}^{n} h_k Z_k,
\]

\( \text{Proc. R. Soc. A} (2011) \)
for some real constants $J_k$ and $h_k$. It can readily be verified that
\[X_k X_{k+1} \propto c_{2k} c_{2(k+1)-1} \quad \text{and} \quad Z_k \propto c_{2k-1} c_{2k},\]
showing that $H_f$ is a quadratic Hamiltonian. Therefore, for every real $t$, the time-evolution operator $e^{it H_f}$ can be written as a (poly-size) matchgate circuit.

The notion of a matchgate-computable Boolean function was introduced in §2. Here, we discuss some simple examples. It can easily be seen that every Boolean function which is either constant or which depends on a single input bit can be computed with unit probability by an elementary matchgate circuit composed of operators $c_m c_n$ and fSWAP gates acting on $n+1$ qubits. Note that the only possible functions of this type are the functions $x \rightarrow 0$, $x \rightarrow 1$, $x \rightarrow x_k$ and $x \rightarrow 1 - x_k$, for some $k$. We show that $x \rightarrow 1 - x_k$ is matchgate-computable with unit probability; the other three cases are treated similarly. For each $k \in [n]$, denote the operator $U_k$ acting on $n+1$ qubits by
\[U_k := c_{2k-1} c_{2(n+1)-1} \propto X_k X_{n+1} \prod_{j=k}^{n} Z_j.\]
Note that $U_k |x, 0\rangle \propto |x_{-k}, 1\rangle$, where $x_{-k}$ denotes the bit string obtained by flipping the $k$th bit of $x$. Now consider an elementary matchgate computation, where first the state $U_k |x, 0\rangle$ is prepared, followed by measurement of qubit $k$. This computation yields the bit $1 - x_k$ with unit probability. This shows that the desired function can be computed with unit probability by applying a suitable matchgate circuit and measuring some qubit in the computational basis. By applying a suitable sequence of fSWAP gates immediately before the measurement, we may assume w.l.o.g. that the first qubit is measured. Indeed, as the measurement is in the computational basis, the minus sign of the fSWAP gate has no relevance, and this gate acts as a simple SWAP.

Remarkably, as we will prove in theorem 2.2, constant and single-bit functions are the only functions that are matchgate-computable with high success probability.

4. Linear threshold gates

In this section, we discuss some elementary features of LTGs. For convenience we recall here their definition. An $n$-bit Boolean function $f$ is an LTG if there exists an $n$-dimensional real vector $w$ and a real number $\theta$, such that
\[(-1)^f(x) = \text{sign}(w^T \hat{x} + \theta)\]
for every $n$-bit string $x$. The pair $(w, \theta)$ is called a representation of $f$. Definition (4.1) has an elementary geometrical interpretation. Taking an arbitrary $w$ and $\theta$, the linear equation $w^T z + \theta = 0$ defines a hyperplane that divides the $n$-dimensional real space into two parts, say $H_+$ and $H_-$, where $H_+$ consists of all $z \in \mathbb{R}^n$, such that $w^T z + \theta \geq 0$ and $H_-$ is defined as the complement of $H_+$. The LTG $f$ associated with $(w, \theta)$ then simply evaluates whether a given $\{\pm 1\}$-vector $\hat{x}$ lies in $H_+$ or $H_-$. Stated differently, a Boolean function $f$ is an LTG iff there exists a hyperplane in $n$-dimensional real space that separates the sets of inputs $x$ that are mapped to 0 and 1, respectively.

It can be easily verified that the constant and single-bit functions are LTGs. Other examples are the \( n \)-bit AND, OR and majority function. The AND gate, for example, has a representation \((w, \theta)\) given by \(w = (1, \ldots, 1)\) and \(\theta = -n + 1/2\). It is also known that not all functions are LTGs. For example, the two-bit parity gate

\[
f(x_1, x_2) := x_1 \oplus x_2
\]  

(4.2)

is not an LTG, as can be easily verified.

Every LTG has infinitely many representations. For example, rescaling the vector \((w, \theta)\) with a positive multiplicative constant trivially leads to the same associated function. We will say that the representation \((w, \theta)\) is normalized if the 1-norm of this vector is equal to 1, i.e. \(\|w\|_1 + |\theta| = 1\). Interestingly, every LTG has a representation \((w, \theta)\), where \(w_k\) and \(\theta\) are integers. The intuition behind this result is the following. It is easy to show that every LTG has a representation \((w, \theta)\), where each \(w_k\) and \(\theta\) are rational numbers, say \(w_k = a_k/b_k\) and \(\theta = c/d\) for suitable integers \(a_k, b_k, c\) and \(d\); this essentially follows from the fact that the rationals are dense in the reals and the property that small perturbations of a representation do not change the associated LTG. Multiplying the rational representation \((w, \theta)\) with the product \(\prod |b_k|/d\) then yields an integer representation.

Further, it is known that every LTG on \(n\) bits has a representation \((w, \theta)\), where each of the components of \(w\), as well as the number \(\theta\), are integers not greater than \(2^N\) in absolute value, with \(N = O(n \log n)\) (Muroga et al. 1961); moreover, there exist LTGs where such large numbers are required (Hastad 1994). This shows that every LTG \(f\) admits a representation that can be fully described in terms of \(O(n^2 \log n)\) bits, and that \(f(x)\) can be evaluated in poly-time when this particular representation is provided.

Finally, we recall that that, given a representation \((w, \theta)\) of an LTG \(f\), the margin of this representation is defined to be the minimal value of \(|w^T \hat{x} + \theta|\) over all \(n\)-bit strings \(x\). The margin \(\epsilon(f) \equiv \epsilon\) of \(f\) is then the maximal margin over all normalized representations. Note that \(\epsilon(f)\), which should in principle be defined as a supremum, is indeed a maximum. This can be argued with standard methods.\(^5\) In §6, we will focus in more detail on the properties of margins of LTGs, which will lead to the proofs of theorems 2.2 and 2.3. Before doing so, we provide the proof of theorem 2.1 in the next section.

5. Proof of theorem 2.1

In this section, we prove theorem 2.1. The proof will proceed in three steps. In step 1, we reduce the study of matchgate-computable functions to the investigation of matrix elements of the form \(\langle x| U^\dagger Z_1 U |x\rangle\), where \(|x\rangle\) denotes a computational basis state, \(U\) is a matchgate circuit and \(Z_1\) is the Pauli Z operator acting on the first qubit. In step 2, which represents the main ingredient

\(^5\)To see this, first note that the margin of a representation \((w, \theta) \equiv z\) is a continuous function of \(z\), being defined as the minimum of a finite number (i.e. \(2^n\)) of continuous functions \(g_z(x) := |w^T \hat{x} + \theta|\) for every \(x\). Thus, \(\epsilon(f)\) is the supremum of a continuous function in \(z\), over all representations \(z\) of \(f\) with \(\|z\|_1 = 1\). As the set of all such normalized representations is a compact set, it follows that the supremum is reached.
of the proof of theorem 2.1, the most general form of such matrix elements is characterized. Finally, in step 3 the proof is completed by combining steps 1 and 2.

(a) Step 1

Let \( f \) be an \( n \)-bit Boolean function, let \( U \) be an arbitrary \( m \)-qubit unitary operation for some \( m \geq n \) and fix \( p \in (0.5,1] \). Furthermore, we denote \( \langle Z \rangle_x := \langle x,0 | U^\dagger Z_1 U | x,0 \rangle \). We now state the following claim.

**Claim.** \( U \) computes \( f \) with probability at least \( p \) if and only if, for every \( x \), one has

(i) \( |\langle Z \rangle_x| \geq 2p - 1 \) and

(ii) \( \text{sign}(\langle Z \rangle_x) = (-1)^{f(x)} \).

To prove this claim, consider the preparation of \( U | x,0 \rangle \) followed by a computational basis measurement of the first qubit and let \( p_x \) denote the probability that the measurement outcome is \( f(x) \), for every \( x \). Then \( U \) computes \( f \) with probability at least \( p \) if and only if \( p_x \geq p \) for every \( x \). We thus have to show that (i) and (ii) are equivalent to the condition \( p_x \geq p \) for all \( x \).

We will distinguish between the cases \( f(x) = 0 \) and \( f(x) = 1 \). We start with the former case. As \( p_x \) and \( 1 - p_x \) are the probabilities of obtaining the measurement outcomes 0 and 1, respectively, one has

\[
\langle Z \rangle_x = p_x - (1 - p_x) = 2p_x - 1.
\]

Now suppose first that \( p_x \geq p \) for every \( x \) (with \( p \in (0.5,1] \) as stated above). Conditions (i) and (ii) then follow immediately. Conversely, assume that (i) and (ii) are true. As (ii) is satisfied, we have \( \langle Z_1 \rangle_x \geq 0 \) and using (i) it thus follows that \( \langle Z \rangle_x \geq 2p - 1 \). Invoking equation (5.1) then implies that \( p_x \geq p \) for every \( x \), as desired. This completes the proof for the case \( f(x) = 0 \).

The case \( f(x) = 1 \) is treated analogously; the main distinction is that now \( p_x \) represents the probability of measuring 1. Consequently, equation (5.1) is replaced by

\[
\langle Z \rangle_x = (1 - p_x) - p_x = 1 - 2p_x.
\]

The remainder of the argument is completely analogous.

(b) Step 2

Conditions (i) and (ii) imply that the study of matchgate-computable functions reduces to the investigation of matrix elements of the form \( \langle x,0 | U^\dagger Z_1 U | x,0 \rangle \), where \( U \) is an arbitrary matchgate circuit. Next, we investigate the most general form which such matrix elements may take. A complete characterization of this problem is obtained in the following theorem.

**Theorem 5.1.** Let \( U \) be an \( n \)-qubit unitary operator. If \( U \) is a matchgate circuit then there exists an \( a \in \mathbb{R}^n \) with \( \| a \|_1 \leq 1 \), such that

\[
\langle x | U^\dagger Z_1 U | x \rangle = a^T \hat{x},
\]

for every \( n \)-bit string \( x \). Conversely, for every \( a \in \mathbb{R}^n \) with \( \| a \|_1 \leq 1 \), there exists an \( n \)-qubit matchgate circuit \( U \), such that equation (5.3) holds.
In the proof of this theorem we will need the following elementary fact.

**Lemma 5.2.** Consider a vector \( a \in \mathbb{R}^n \) with \( \|a\|_1 \leq 1 \). Then there exist \( u, v \in \mathbb{R}^n \) with \( \|u\|_2 = 1 \) and \( \|v\|_2 \leq 1 \), such that \( a_k = u_k v_k \) for every \( k \in [n] \).

**Proof.** Define \( u \) and \( v \) by

\[
u_k := \frac{|a_k|}{\|a\|_1} \quad \text{and} \quad v_k := \sqrt{|a_k| \cdot \|a\|_1} \cdot \text{sign}(a_k), \tag{5.4}
\]

for every \( k \in [n] \), respectively. Obviously, \( a_k = u_k v_k \). Moreover, \( \|u\|_2 = 1 \) and \( \|v\|_2 \leq \|a\|_1 \leq 1 \), as can be easily verified. This proves the lemma.

**Proof of theorem 5.1.** We first prove the forward direction. Denote \( O := U^\dagger Z_1 U \) and let \( R \) be the \( SO(2n) \) rotation associated to \( U \) via equation (3.2). Letting \( \rho \) and \( \rho' \) denote the first, respectively, second, row of \( R \) and using that \( Z_1 = -ic_1 c_2 \), it follows that

\[
O = -i[U^\dagger c_1 U][U^\dagger c_2 U] = \sum \rho_\mu \rho'_\nu [-ic_\mu c_\nu], \tag{5.5}
\]

where the sum is over all \( \mu, \nu \in [2n] \). As \( \langle x|O|x \rangle \) is a diagonal entry of \( O \) for every \( x \), we only need to focus on the diagonal part of this operator, i.e. \( \text{diag}(O) := \sum_x \langle x|O|x \rangle \langle x|x \rangle \). Using the explicit representation (3.1) of the \( c_\mu \), it is easily verified that

\[
\text{diag}(-ic_\mu c_\nu) = \begin{cases}
-iI & \text{if } \mu = \nu, \\
Z_k & \text{if } (\mu, \nu) = (2k - 1, 2k) \text{ for some } k \in [n], \\
-Z_k & \text{if } (\mu, \nu) = (2k, 2k - 1) \text{ for some } k \in [n], \\
0 & \text{otherwise}.
\end{cases} \tag{5.6}
\]

Setting \( a_k := \rho_{2k-1} \rho'_{2k} - \rho_{2k} \rho'_{2k-1} \) for every \( k \in [n] \) and using that \( \sum_\mu \rho_\mu \rho'_\mu \) is zero since \( \rho \) and \( \rho' \) are two distinct rows of an orthogonal matrix, it follows that

\[
\text{diag}(O) = \sum_{k=1}^n a_k Z_k. \tag{5.7}
\]

The \( \langle x, x \rangle \) diagonal entry of \( O \) thus reads:

\[
\langle x|O|x \rangle = \sum_{k=1}^n a_k \langle x|Z_k|x \rangle = a^T \hat{x}. \tag{5.8}
\]

This shows that equation (5.3) is satisfied. Note also that \( |\langle x|O|x \rangle| \leq 1 \) for every \( x \) since \( O \) is unitary. Moreover, it is easily verified that there exists an \( x \) such that \( a^T \hat{x} = \|a\|_1 \). This shows that \( \|a\|_1 \leq 1 \).

To prove the reverse direction, consider an arbitrary \( a \in \mathbb{R}^n \) with \( \|a\|_1 \leq 1 \). Owing to lemma 5.2, there exist \( n \)-dimensional real vectors \( u \) and \( v \) with \( \|u\|_2 = 1 \) and \( \|v\|_2 \leq 1 \), such that \( a_k = u_k v_k \) for every \( k \in [n] \). Furthermore, it is elementary that for every such \( u \) and \( v \) there exists a vector \( w \in \mathbb{R}^n \) that is orthogonal to \( u \) and that satisfies \( \|w\|_2^2 = 1 - \|v\|_2^2 \). Consequently, the \( 2n \)-dimensional vectors

\[
\rho := (u_1, 0, u_2, 0, \ldots, u_n, 0) \quad \text{and} \quad \rho' := (w_1, v_1, w_2, v_2, \ldots, w_n, v_n) \tag{5.9}
\]

are unit vectors (w.r.t. the 2-norm) that are orthogonal. Let \( R \) be any \( SO(2n) \) rotation having \( \rho \) and \( \rho' \) as first, respectively, second row. Let \( U \) be the \( n \)-qubit
matchgate circuit associated to $R$. Analogous to the proof of the forward direction of the theorem, a direct calculation shows that the diagonal part of $U^\dagger Z_1 U$ equals

$$\sum (\rho_{2k-1} \rho_{2k}' - \rho_{2k} \rho_{2k-1}') Z_k = \sum_{k=1}^n a_k Z_k.$$  

(5.10)

It immediately follows that equation (5.3) is satisfied. This completes the proof.

(c) Step 3

We now show how the above result leads to the proof of theorem 2.1. Invoking step 1, it suffices to show that, for every $n$-bit Boolean function $f$ and $p \in (0.5, 1]$, the following are equivalent:

— There exists an $m$-qubit matchgate circuit $U$, for some $m \geq n$, such that conditions (i) and (ii) in step 1 hold;
— $f$ is an LTG with margin $\epsilon \geq 2p - 1$.

We first prove the forward direction of the claim. Let $U$ be a matchgate circuit on $m$ qubits, such that (i) and (ii) hold. We first invoke theorem 5.1. This yields a vector $\tilde{a} := (a_1, \ldots, a_n)$ and $b := \sum_{l=n+1}^m a_l$, it then immediately follows that

$$\langle x, 0 | U^\dagger Z_1 U | x, 0 \rangle = \tilde{a}^T \hat{x} + b,$$

(5.11)

for every $n$-bit string $x$. Together with condition (ii) in step 1, this shows that $f$ is an LTG with representation $(\tilde{a}, b)$. Normalizing the vector $(\tilde{a}, b)$ w.r.t. the 1-norm yields a normalized representation $w := \gamma \tilde{a}$ and $\theta := \gamma b$, where $\gamma^{-1} := \|\tilde{a}\|_1 + |b|$. Note that $\gamma^{-1} \leq \|a\|_1 \leq 1$. Using equation (5.11) and condition (i) of step 1 it follows that

$$|\tilde{a}^T \hat{x} + b| \geq 2p - 1.$$  

(5.12)

Moreover, using the definitions of $w$ and $\theta$ and the fact that $\gamma \geq 1$, it finally follows that

$$|w^T \hat{x} + \theta| \geq \gamma (2p - 1) \geq 2p - 1,$$

(5.13)

for every $x$. This shows that the margin of $f$ is at least $2p - 1$.

We now show the converse. Consider an $n$-bit LTG $f$. Let $\epsilon \in (0, 1]$ be its margin with associated (normalized) representation $(w, \theta)$ and denote $p := (\epsilon + 1)/2$. Owing to theorem 5.1, there exists an $(n + 1)$-qubit matchgate circuit $U$, such that

$$\langle x, y | U^\dagger Z_1 U | x, y \rangle = w^T \hat{x} + \theta \hat{y},$$

(5.14)

for every $n$-bit string $x$ and for every $y = 0, 1$. This readily implies that

$$\text{sign}(\langle x, 0 | U^\dagger Z_1 U | x, 0 \rangle) = \text{sign}(w^T \hat{x} + \theta) = (-1)^{f(x)},$$

(5.15)

for every $x$. Moreover, as $\epsilon$ is the margin of $f$, it follows that

$$|\langle x, 0 | U^\dagger Z_1 U | x, 0 \rangle| = |w^T \hat{x} + \theta| \geq 2p - 1,$$

(5.16)

for every $x$. This shows that conditions (i) and (ii) in step 1 are fulfilled. This completes the proof of theorem 2.1.
Remark 5.3. It follows from the above argument that an \( n \)-bit Boolean function \( f \) is computable by an \( m \)-qubit matchgate circuit with probability at least \( p \), for some \( m \geq n \), if and only if \( f \) is computable with probability at least \( p \) by a matchgate circuit acting on at most \( n + 1 \) qubits.

6. Margins of threshold gates

In this section, we analyse the properties of margins of LTGs in more detail. In particular, the proofs of theorems 2.2 and 2.3 will follow from the considerations in this section.

(a) Large margins

Next, we investigate the subclass of LTGs with large margin. We will in particular show that any LTG with margin strictly larger than \( 1/2 \) is essentially trivial. The proof of theorem 2.2 will follow immediately from this property.

Recall that, formally, a Boolean function \( f \) on \( n \) bits is said to depend on its \( k \)th variable, if there exists an \( n \)-bit string \( x \), such that \( f(x) \neq f(x_{\neg k}) \), where \( x_{\neg k} \) is the string obtained by flipping the \( k \)th bit of \( x \). We can now state the following result:

Lemma 6.1. Any LTG with margin \( \epsilon \) can depend on at most \( t = 1/\epsilon \) of its variables.

Proof. Let \( f \) be an \( n \)-bit LTG and let \( \epsilon \) be the margin of \( f \) with associated normalized representation \((w, \theta)\). We make the following claim. **Claim:** if \( f \) depends on its \( k \)th variable then \( |w_k| \geq \epsilon \). The proof of the lemma immediately follows from correctness of this claim, by using that \( \|w\|_1 \leq 1 \) as \((w, \theta)\) is a normalized representation. We now prove the claim. For simplicity but w.l.o.g., we set \( k := 1 \) and assume that \( f \) depends on its first variable. We prove that \( |w_1| \geq \epsilon \). Denote \( \tilde{w} := (w_2, \ldots, w_n) \). If \( f \) depends on its first variable, there must exist an \( \tilde{s} \in \{\pm 1\}^{n-1} \), such that \( \tilde{w}^T \tilde{s} \pm |w_1| + \theta \) have opposite signs. We consider the following two possibilities: (a) \( \tilde{w}^T \tilde{s} + \theta \geq 0 \) or (b) \( \tilde{w}^T \tilde{s} + \theta \leq 0 \). In case (a), it follows that \( \tilde{w}^T \tilde{s} + |w_1| + \theta \geq 0 \), and hence we must have \( \tilde{w}^T \tilde{s} - |w_1| + \theta \leq 0 \). Since \( \epsilon \) is the margin of \((w, \theta)\), it follows that

\[
\tilde{w}^T \tilde{s} - |w_1| + \theta \leq -\epsilon.
\]

Hence, \( |w_1| \geq \epsilon \). Case (b) is treated analogously.

It follows that any LTG that depends on all its \( n \) variables can admit a margin of size at most \( 1/n \), and any LTG with constant margin can depend on at most a constant number of its input bits. What is more, if \( \epsilon \) is sufficiently close to 1 viz. \( \epsilon > 1/2 \), then \( f \) can depend on at most one of its variables. Indeed, it follows from lemma 6.1 that \( f \) can depend on at most \( t = \epsilon^{-1} < 2 \) input bits, i.e. \( t \) is 0 (corresponding to a constant function) or 1. Combining these considerations with theorem 2.1, the forward direction of theorem 2.2 follows immediately: indeed, owing to theorem 2.1, any Boolean function which is matchgate-computable with probability \( p > 3/4 \) must be an LTG with margin \( \epsilon > 1/2 \), and hence of the form indicated. The proof of the converse direction of theorem 2.2 is elementary, as discussed in §3.

More general than theorem 2.2, we have actually shown that any function which can be computed by a matchgate circuit with success probability at least \( p \) is an LTG that depends on at most \( O(p^{-1}) \) of its input bits. As a consequence, whenever a constant success probability is considered (i.e. independent of the input size), only functions can be computed that depend on a constant number of input bits. Conversely, we have proved that any LTG depending on \( k \) of its input bits can be computed by a matchgate circuit with success probability of at most \( (1/2) + O(k^{-1}) \). Therefore, any LTG that depends on all its \( n \) input bits can be computed by a matchgate circuit with probability at most \( (1/2) + O(n^{-1}) \), which always lies at least polynomially close to 0.5.

Remark 6.2 (relation to Jozsa et al. (2010)). As shown above, if \( p = O(1) \) then matchgate circuits \( U \) can merely compute functions \( f(x) \) that depend on \( O(1) \) input bits, i.e. bounded-error matchgate computations have a rather limited power. It is interesting to compare with the study of Jozsa et al. (2010). In order to understand the relation between Jozsa et al. (2010) and the present work it is important to remark that in the study of Jozsa et al. (2010), one considers matchgate circuits \( U \equiv U_x \) which may depend, via an arbitrary log-space classical computation, on the entire input \( x \). This definition thus effectively supplements matchgate circuits with the power of log-space classical computation. Within this setting, it was shown that the class of problems computable with bounded error by such log-space-generated matchgate circuits \( U_x \) is non-trivial, coinciding with the class of all problems computable with a quantum computer acting on \( O(\log n) \) qubits. In contrast, in the present work we always consider matchgate circuits that depend only on the size of the input, i.e. one circuit \( U \equiv U_n \) takes all inputs \( x \) of size \( |x| = n \), as commonly done. The feature that bounded-error matchgate computations have such limited power in our work, whereas in Jozsa et al. (2010) they are equivalent to the entire class of quantum log-space computations thus seems to be an intriguing manifestation of the \( U_n \leftrightarrow U_x \) distinction.

We conclude this section with an example. Let \( n \) be odd and let \( f_{\text{maj}} \) denote the majority function on \( n \) bits, i.e. \( f_{\text{maj}}(x) \) is 0 iff the \( n \)-bit string \( x \) contains more zeros than ones. It can easily be verified that \( f_{\text{maj}} \) is an LTG with normalized representation \( (w, \theta) \) defined by \( w_k := n^{-1} \) for every \( k \) and \( \theta := 0 \). Moreover, the minimal value of \( |w^T x + \theta| \) over all \( x \) is easily shown to be \( n^{-1} \), showing that \( n^{-1} \) is a lower bound for the margin of \( f_{\text{maj}} \). As \( f_{\text{maj}} \) depends on all its \( n \) variables, its margin is at most \( n^{-1} \) owing to lemma 6.1. This shows that the margin of the majority function is precisely \( n^{-1} \equiv e_{\text{maj}} \). Owing to theorem 2.1, there hence exists a matchgate circuit that computes this function with probability

\[
p_{\text{maj}} = \frac{e_{\text{maj}} + 1}{2} = \frac{1}{2} + \frac{1}{2n}.
\]

Moreover, any matchgate circuit computing the majority function can do so with probability at most \( p_{\text{maj}} \).

(b) Margins and integer representations

Next, we focus on the possible types of asymptotic behaviour that the margins of a family of LTGs may exhibit. We will in particular be interested in the distinction between margins that are polynomially bounded and margins that are
exponentially small in the input size. As discussed in §2, the subclass of (families of) LTGs with polynomially bounded margin coincides with those functions that are matchgate-computable with poly-bounded error. In the following, we will in particular prove a simple characterization of the families of LTGs with poly-bounded margin.

An important parameter of an LTG \( f \) in the present context will be the integer weight \( \omega(f) \equiv \omega \) of \( f \), defined to be the minimal 1-norm \( \| w \|_1 + |\theta| \) of any possible integer representation of \( f \). A family of LTGs \( \{ f_n : n = 1, 2, \ldots \} \), where \( f_n \) acts on \( n \) bits, is said to have polynomial integer weight if the integer weight \( \omega_n \) of \( f_n \) scales polynomially with \( n \). Interestingly, it turns out that the margin of an LTG and its integer weight are closely related concepts:

**Theorem 6.3.** Consider an \( n \)-bit LTG with margin \( \epsilon \) and integer weight \( \omega \). Then

\[
\frac{1}{\epsilon} \leq \omega \leq 2 \cdot \frac{n + 1}{\epsilon}. \tag{6.3}
\]

Note that, in the case of large \( n \), the second inequality in equation (6.3) simplifies to \( \omega \leq O(n/\epsilon) \). As an immediate corollary of theorem 6.3, the following property follows:

A family of LTGs has poly-bounded margin if and only if it has polynomial integer weight.

Combining this result with theorem 2.1 then proves theorem 2.3.

**Proof of theorem 6.3.** We first prove the first inequality. Let \( (v, \varphi) \) be an integer representation with \( \| v \|_1 + |\varphi| = \omega \). Normalizing \( (v, \varphi) \) leads to the representation \( (\hat{w}, \theta) \) defined by \( w := \omega^{-1} v \) and \( \theta = \omega^{-1} \varphi \). We claim that \( (\hat{w}, \theta) \) has margin at least \( \omega^{-1} \), implying that \( \epsilon \geq \omega^{-1} \) as desired. To prove the claim, note that the sign of \( v^T \hat{x} + \theta \) equals \( (-1)^{f(x)} \) for every \( n \)-bit string \( x \). This implies that \( v^T \hat{x} + \varphi \neq 0 \) for any \( x \). As the components of \( v \) and \( \varphi \) are integers, \( v^T \hat{x} + \varphi \) is an integer as well for any \( x \). Hence, the property \( v^T \hat{x} + \varphi \neq 0 \) implies that \( |v^T \hat{x} + \varphi| \geq 1 \). It follows that \( |w^T \hat{x} + \theta| \geq \omega^{-1} \), i.e. the margin of \( (\hat{w}, \theta) \) is at least \( \omega^{-1} \).

Next, we prove the second inequality. Let \( (w, \theta) \) be a normalized representation of \( f \) with margin \( \epsilon \). Let \( d \) be a positive integer; for now \( d \) is arbitrary but we will fix a value later. Let \( w_{k\mu} \) and \( \theta_{\mu} \) represent the \( \mu \)th bit in the binary expansion\(^6\) of \( w_k \) and \( \theta \), respectively. Now let \( v_k \) and \( \varphi \) be the rational numbers obtained by truncating the binary expansion of \( w_k \), respectively, \( \theta \), after the \( d \)th bit (and keeping the same overall signs). That is, we define \( v_k = \text{sign}(w_k) \sum w_{k\mu} 2^{-\mu} \) and \( \varphi = \text{sign}(\theta) \sum \theta_{\mu} 2^{-\mu} \) for every \( k \), where the sums run from 1 to \( d \). Note that

\[
\| v \|_1 + |\varphi| \leq \| w \|_1 + |\theta| = 1. \tag{6.4}
\]

It further follows from the definitions of \( v \) and \( \varphi \) that \( |w_k - v_k| \leq 2^{-d} \) and \( |\varphi - \theta| \leq 2^{-d} \). This implies that

\[
|(v - w)^T \hat{x} + (\varphi - \theta)| \leq (n + 1) 2^{-d}. \tag{6.5}
\]

\(^6\)Any real number \( a \in [1, -1] \) can be expanded in a unique way as \( a = \text{sign}(a) \sum_{\mu=1}^{\infty} a_{\mu} 2^{-\mu} \), where each \( a_{\mu} \in \{0, 1\} \).

We now choose \( d \) to be the smallest positive integer, such that \((n+1)2^{-d}\) is strictly smaller than \( \epsilon \). Then, as \( |w^T \hat{x} + \theta| \geq \epsilon \), the quantity

\[
w^T \hat{x} + \theta + \{(v - w)^T \hat{x} + (\varphi - \theta)\},
\]

must have the same sign as \( w^T \hat{x} + \theta \) for every \( x \). Note that equation (6.6) coincides with \( v^T \hat{x} + \theta \) for every \( x \). This shows that \((v, \varphi)\) is also a representation of \( f \). But then also multiplying \((v, \varphi)\) with \( 2^d \) leads to a representation of \( f \). The latter representation is integer, and moreover has 1-norm at most \( 2^d \), since the 1-norm of \((v, \varphi)\) is at most 1 owing to equation (6.4). This shows that the integer weight of \( f \) is at most \( 2^d \). Finally, for our choice of \( d \) one has

\[
2^d \leq 2 \cdot \frac{n + 1}{\epsilon}.
\]

(6.7)

To see this, remark that \( d \) is defined to be the smallest integer strictly larger than \( \log_2[(n + 1)/\epsilon] \). But then \( d \) must satisfy

\[
d \leq \log_2 \left( \frac{n + 1}{\epsilon} \right) + 1,
\]

(6.8)

which is equivalent to equation (6.7). This proves the second inequality in equation (6.3).

7. An equivalent classical computer

Theorem 2.1 connects the optimal success probability \( p \) of computing a linear threshold function \( f \) with any matchgate circuit with the margin \( \epsilon \) of this LTG. This is a somewhat peculiar connection, e.g. since the definition of the margin of an LTG \emph{a priori} does not seem to have anything to do with probabilities. In order to understand this relation better, in this section we construct a very simple class of classical computers that are capable of (probabilistically) computing LTGs with precisely the same relation between \( p \) and \( \epsilon \).

To motivate this class, we reiterate the following simple example that was discussed in §2. Let \( f_{\text{maj}} \) denote the \( n \)-bit majority function as before, and let \( \epsilon := n^{-1} \) be its margin. Owing to theorem 2.1, there exists a matchgate circuit that computes this function with probability \( p_{\text{maj}} \) defined in equation (6.2), and this is the optimal success probability that any matchgate circuit can achieve. Now consider the following elementary classical computation, consisting of the following steps:

- Choose an \( n \)-bit input string \( x \).
- Generate a random integer \( k \) between 1 and \( n \).
- Output the bit value \( x_k \).

We now claim that, for every \( x \), the output of this computation is \( f_{\text{maj}}(x) \) with probability at least \( p_{\text{maj}} \). To see this, note that the probability \( p_x \) that the above
procedure outputs 0 is given by

\[ p_x = \frac{|\{k \in [n] : x_k = 0\}|}{n}, \quad (7.1) \]

and the probability of outputting 1 is \( q_x = 1 - p_x \). If \( x \) contains more zeros than ones—i.e. if \( f_{\text{maj}}(x) \) is zero—then the probability \( p_x \) is at least \( p_{\text{maj}} \), as can easily be verified. Similarly, if \( x \) contains more ones than zeros, \( q_x \) is at least \( p_{\text{maj}} \) as well. Thus, for any \( x \) the output of the computation is \( f_{\text{maj}}(x) \) with probability at least \( p_{\text{maj}} \). In other words, the above classical computation computes the majority function with the same probability of success which can be achieved by the optimal matchgate circuit. Next, we will show that every LTG \( f \) with margin \( \epsilon \) can be associated with a classical computation of the above nature.

The relevant class of classical computations is defined as follows. Fix a probability distribution \( P := \{\pi_k\} \) on the set of integers from 1 to \( n+1 \), together with a string \( c \) of \( n+1 \) bits. We define the weighted majority sampling (WMS) computation associated with \( P \) and \( c \) to consist of the following steps:

— Choose an \( n \)-bit input string \( x \).
— Sample from the distribution \( P \), yielding \( k \in [n+1] \) with probability \( \pi_k \).
— If \( k \leq n \) then output the bit \( z_{\text{out}} := x_k \oplus c_k \). If \( k = n+1 \) then output \( z_{\text{out}} := c_{n+1} \).

We say that an \( n \)-bit Boolean function \( f \) is WMS-computable with probability at least \( p \) if there exist \( P \) and \( c \), such that the above three-step procedure yields the output \( z_{\text{out}} = f(x) \) with probability at least \( p \) for every \( n \)-bit input \( x \). We prove that the classes of WMS-computable and matchgate-computable functions precisely coincide.

**Claim.** Let \( p \in (0.5, 1] \). A function is matchgate-computable with probability at least \( p \) iff this function is WMS-computable with probability at least \( p \).

Consider a WMS computation with associated \( P \) and \( c \). It will be convenient to consider a slightly modified computation, where the output is \( \hat{z}_{\text{out}} = (-1)^z_{\text{out}} = \pm 1 \) instead of the bit \( z_{\text{out}} \). This will facilitate notation in the proof (but does not play any essential role otherwise). Further, we let \( \langle \hat{z}_{\text{out}} \rangle_x \) denote the expected value of \( \hat{z}_{\text{out}} \) given that \( x \) is the input of the computation.

We now prove the claim. Let \( f \) be an arbitrary \( n \)-bit Boolean function. It follows from §5a that \( f \) is matchgate-computable with probability at least \( p \) iff there exists a matchgate circuit \( \hat{U} \) acting on \( m \geq n \) qubits such that, for every \( x \), one has

(a) \(|\langle Z \rangle_x| \geq 2p - 1 \) and
(b) \( \text{sign}(Z)_x = (-1)^f(x) \).

Furthermore, using an argument analogous to that in §5a, it can easily be shown that \( f \) is WMS-computable with probability at least \( p \) if and only if there exist \( P \) and \( c \) such that, for every \( x \), one has

(a′) \(|\langle \hat{z}_{\text{out}} \rangle_x| \geq 2p - 1 \) and
(b′) \( \text{sign}(\hat{z}_{\text{out}})_x = (-1)^f(x) \),
for every $x$. We thus have to prove that, for every function, conditions (a) and (b) hold for some matchgate circuit $U$ iff (a’) and (b’) hold for some $P$ and $c$.

Suppose first that (a’) and (b’) are satisfied for some $P$ and $c$. We define $w \in \mathbb{R}^n$ and $q \in \mathbb{R}$ by

$$w_k := (-1)^{c_k} \pi_k \quad \text{and} \quad \theta := (-1)^{c_{n+1}} \pi_{n+1},$$

(7.2) for every $k \in [n]$. Note that the vector $(w, \theta)$ has unit 1-norm. Now let $x$ be an arbitrary bit string and run the WMS computation as described above. Then the expected value of $\hat{z}_{\text{out}}$ is

$$\langle \hat{z}_{\text{out}} \rangle_x = \left\{ \sum_{k=1}^n \pi_k (-1)^{x_k+\pi_k} \right\} + \pi_{n+1} (-1)^{c_m} = w^T \hat{\chi} + \theta.$$  

(7.3)

Owing to theorem 5.1, there exists a matchgate circuit $U$ on $n+1$ qubits such that

$$\langle Z_1 \rangle_x := \langle x, 0 | U^\dagger Z_1 U | x, 0 \rangle = w^T \hat{\chi} + \theta = \langle \hat{z}_{\text{out}} \rangle_x.$$  

(7.4)

As $\langle Z_1 \rangle_x = \langle \hat{z}_{\text{out}} \rangle_x$ for every $x$, it follows that conditions (a) and (b) are satisfied for $U$.

To prove the converse, consider an $m$-qubit matchgate circuit $U$ such that (a) and (b) hold. Owing to theorem 5.1, there exists $(v, \varphi)$ with 1-norm at most 1, such that

$$\langle Z_1 \rangle_x = \langle x, 0 | U^\dagger Z_1 U | x, 0 \rangle = v^T \hat{\chi} + \varphi,$$  

(7.5)

for every $n$-bit string $x$. Normalizing $(v, \varphi)$ w.r.t. the 1-norm yields a normalized representation $w := \gamma v$ and $\theta := \gamma \varphi$, where $\gamma^{-1} := \|v\|_1 + |\varphi|$. Note that $\gamma^{-1} \leq 1$. Now choose $P$ and $c$ such that equation (7.2) is satisfied. Using an argument similar to the first part of the proof, the expected value of the associated WMS computation is $\langle \hat{z}_{\text{out}} \rangle_x = w^T \hat{\chi} + \theta$. We thus have

$$\langle \hat{z}_{\text{out}} \rangle_x = \gamma (v^T \hat{\chi} + \varphi) = \gamma \langle Z_1 \rangle_x$$  

(7.6)

for every $x$, where $\gamma \geq 1$. Using the identity $\langle \hat{z}_{\text{out}} \rangle_x = \gamma (Z_1) \langle x \rangle_x$, and the fact that (a) and (b) hold, it immediately follows that (a’) and (b’) are satisfied for $(P, c)$.

The author is grateful to S. Bravyi, I. Cirac, R. Jozsa, C. Kraus and K. Vollbrecht for discussions. Work supported by the excellence cluster MAP.

References


