Distillation with sublogarithmic overhead

Matthew B. Hastings$^{1,2}$ and Jeongwan Haah$^2$

$^1$Station Q, Microsoft Research, Santa Barbara, CA 93106-6105, USA
$^2$Station Q Quantum Architectures and Computation, Microsoft Research, Redmond, WA 98052, USA

It has been conjectured [1] that for any distillation protocol for magic states for the $T$ gate, the number of noisy input magic states required per output magic state at output error rate $\epsilon$ is $\Omega(\log(1/\epsilon))$. We show that this conjecture is false. We find a family of quantum error correcting codes of parameters $[\sum_{m=0}^r (\binom{m}{i}), \sum_{m=0}^r (\binom{m}{i}^+)\binom{r+i}{i}]$ for any integers $m > 2r$, $r > w \geq 0$, by puncturing quantum Reed-Muller codes. When $m > vr$, our code admits a transversal logical gate at the $\nu$-th level of Clifford hierarchy. In a distillation protocol for magic states at the level $\nu = 3$ ($T$-gate), the ratio of input to output magic states is $O(\log^7(1/\epsilon))$ where $\gamma = \log(n/k)/\log(d) < 0.678$ for some $m, r, w$. The smallest code in our family for which $\gamma < 1$ is on $\approx 2^{28}$ qubits.

I. INTRODUCTION

One of the most promising paths towards a scalable quantum computer involves implementing very high accuracy Clifford operations, and using them to perform magic state distillation [2, 3], turning a large number of noisy $T$ gates into a small number of $T$ gates with some small error $\epsilon_{out}$. This magic state distillation is estimated to be the major source of overhead, and is thus of great theoretical and practical importance.

Assuming perfect Clifffords, three previous protocols [4,6] enabled magic state distillation with a ratio of input to output magic states which is $O(\log^2(1/\epsilon_{out}))$ as $\epsilon_{out} \rightarrow 0$ for $\gamma$ arbitrarily close to 1. It has been conjectured [1] that $\gamma > 1$ for all protocols.

Given an $[n, k, d]$ error correcting code admitting a transversal $T$ gate, then using noisy magic states of error rate $\epsilon_{in}$ one can output $k$ magic states of error rate $O(n\epsilon_{in})$. Concatenating $z$ times, one obtains $k^z$ magic states of error rate $\epsilon_{out} = O(n^z\epsilon_{in}^z)$ from $n^z$ noisy magic states. For a fixed ratio, a code of input to output magic states is thus $O(\log^2(1/\epsilon_{out}))$ where $\gamma = \frac{\log(n/k)}{\log(d)}$.

We find quantum error correcting codes with $\gamma$ asymptotically approaching 0.6779⋅⋅⋅.

II. DEFINITIONS, RESULTS AND PROOFS

For any non-negative integers $m \geq r$, let $RM(r, m)$ denote the classical Reed-Muller code on $2^m$ bits; a codeword of $RM(r, m)$ is a complete list of function values $(f(v) : v \in \mathbb{F}_2^m) \in \mathbb{F}_2^m$ where $f$ is a polynomial of degree at most $r$ in $m$ binary variables $x_i = x^i$. We will not distinguish the list of function values from the function itself. If $m > vr$, then every codeword of $RM(r, m)$ has weight divisible by $2^r$ [7]. It is also well-known that $\dim \mathbb{F}_2^r RM(r, m) = \sum_{i=0}^r (\binom{m}{i}) = (\binom{m}{r})$, $RM(r, m)^⊥ = RM(m-r-1, m)$, and the minimum distance of $RM(r, m)$ is $2^{m-r}$ [8].

Let $|w|$ denote the number of 1’s in $v \in \mathbb{F}_2^m$ (Hamming weight). For any integer $w < m$, let $PRM(r, m, w)$ denote the punctured Reed-Muller code by forgetting coordinates $v$ with $|v| \leq w$; a codeword of $PRM(r, m, w)$ is a list of function values $(f(v) : v \in \mathbb{F}_2^m$ and $|v| > w)$ of a degree-$r$ polynomial $f$. The codeword length is $\sum_{m=0}^r (\binom{m}{i})$.

If $w < 0$, then $PRM(r, m, w) = RM(r, m)$. The dual of $PRM(m-r-1, m, w)$ is a shortened Reed-Muller code $SRM(r, m, w)$, whose codewords are still of form $(f(v) : v \in \mathbb{F}_2^m$ and $|v| > w)$ but the polynomial function has to vanish on the punctured coordinates: $f(v) = 0$ if $|v| \leq w$ [8]. Hence, $SRM(r, m, w) = PRM(m-r-1, m, w)^⊥ \subseteq PRM(r, m, w)$. The minimum distance of $SRM(r, m, w)$ is $2^{m-r}$ if $w < r$.

Theorem 1. Let $w, r, m$ be integers such that $0 \leq 2w < 2r < m$. Consider a quantum CSS code $Q$ whose X-stabilizer group is given by $SRM(r, m, w)$, and Z-stabilizer group by $SRM(m-r-1, m, w)$. Then, $Q$ is a $[\{m = (m, w), k = (m, w), d = (r+1)\}]$ code, and if $m > vr$ for some positive integer $\nu$, there exists a choice of logical operators such that a transversal gate $\bigotimes_{i=1}^n \text{diag}(1, \exp(2\pi i/2w))$ becomes a logical operator that is the product of diag$(1, \exp(-2\pi i/2w))$ over all logical qubits.

Proof. The code length is obvious by definition. We need the following lemma before proving the values of $k, d$:

Lemma 1. Given $f : \mathbb{F}_2^m \rightarrow \mathbb{F}_2$, let $|f|_w$ be the number of $v \in \mathbb{F}_2^m$ such that $|f(v)| = 1$ and $|v| > w$. Let $D(r, m, w) = \min_{f\in RM(r, m), f \neq 0} |f|_w$.

Then, $D(r, m, w) = (m-r)_w$. In particular, if $m-r > w$, the minimum distance of $PRM(r, m, w)$ is $(m-r)_w$, and there is no nonzero polynomial function of degree at most $r$ supported on $\{v \in \mathbb{F}_2^m : |v| \leq w\}$.

Proof. The polynomial function $(1+x_1)\cdots(1+x_r) \in RM(r, m)$, has $|f|_w = (m-r)_w$. We show it is the minimum by induction on $m$. The base case $m = 0$ is clear since $D(0, 0, w < 0) = 1$ and $D(0, 0, w \geq 0) = 0$. Now let $m > 0$ and assume $D(r, m-1, w) = (m-r-1)_w$ for all $0 \leq r < m-1$ and any $w$.

For $r = 0$ or $r = m$, it is obvious that $D(r, m, w) = (m-r)_w$. For $0 < r < m$, we use the inductive hypothesis and the recursive construction of Reed-Muller codes; namely, any polynomial function $f$ in $x_1, \ldots, x_m$ of $RM(r, m)$ can be written as
\[ f(x_1, \ldots, x_m) = g(x_1, \ldots, x_{m-1}) + x_m h(x_1, \ldots, x_{m-1}) \]

where \( g \in \text{RM}(r, m - 1) \) and \( h \in \text{RM}(r - 1, m - 1) \). To find a lower bound on \( |f|_{>w} \), we separate cases where \( h = 0 \) and \( h \neq 0 \). If \( h = 0 \), then \( |f|_{>w} = |g|_{>w} + |g|_{>w-1} \) where \( |g|_{>w} \) is when \( x_m = 0 \) and \( |g|_{>w-1} \) is when \( x_m = 1 \). (Here, the domain of \( g \) and \( h \) is \( \mathbb{F}_2^{m-1} \).) Hence, \( |f|_{>w} \geq D(r, m - 1, w) + D(r, m - 1, w - 1) \). If \( h \neq 0 \), then by a triangle inequality we have \( |g + h|_{>w} \geq |h|_{>w} - |g|_{>w} \), implying that \( |f|_{>w} = |g|_{>w} + |g + h|_{>w} \) is when \( |h|_{>w} \geq D(r - 1, m - 1, w) \). Therefore,

\[
D(r, m, w) \geq \min\left(\frac{D(r, m - 1, w) + D(r, m - 1, w - 1)}{D(r - 1, m - 1, w)}\right)
\]

where the last equality follows by the Pascal identity on the binomial coefficients.

To find the desired set of logical operators, we represent \( \text{PRM}(r, m, w) \), the set of all X-logical operators including X-stabilizers, as the span of the rows of \( G_T \) and \( G_0 \) where

\[
\begin{bmatrix}
I_k \\
G_T \\
0
\end{bmatrix}
\]

is the generating matrix for \( \text{RM}(r, m) \) obtained by bringing punctured coordinates (there are \( k = \binom{m}{\leq w} \)) to the left by permutation of columns, and Gaussian elimination on the rows. The fact that the top-left submatrix is the full rank identity matrix is due to the lemma, since, otherwise, the submatrix would have a nonzero right kernel, which is impossible because any nonzero vector in the dual of \( \text{RM}(r, m) \) is not supported on the punctured coordinates. The desired basis of the logical operators is given by \( G_T \); declare that each row of \( G_T \) corresponds to a pair of X- and Z-logical operators. This gives the correct commutation relations, and thus the number of logical qubits is \( \binom{m}{\leq w} \).

The dual of the X-stabilizer space is \( \text{PRM}(m - r - 1, m, w) \), and hence the minimum of the weight of any Z-logical operator is \( \binom{m}{< w} \). The dual of the Z-stabilizer space is \( \text{PRM}(r, m, w) \), and hence the minimum of the weight of any X-logical operator is \( \binom{m-r}{< w} \). Thus, \( d \geq \binom{m-r}{< w} \). In fact, \( d = \binom{m-r}{< w} \) because any stabilizer belongs to either \( \text{SRM}(r, m, w) \) or \( \text{SRM}(m - r - 1, m, w) \), and hence has weight \( \geq 2^{r+1} > \binom{m-r}{< w} \) or zero.

The transversality of the logical operators can be computed easily by working with state vector directly. See [4]. One should use the fact that any set of \( \ell \geq 2 \) distinct rows of \( \begin{bmatrix} G_T \\ G_0 \end{bmatrix} \) have overlap that is a multiple of \( 2^{\ell-1} \). \( \square \)

**Corollary 1.** There exist quantum codes of parameters \([n, k, \ell]\) admitting transversal logical gate \( T = \text{diag}(1, e^{i\pi/4}) \) simultaneously on every logical qubit with \( \gamma = \log(n/k)/\log d \) arbitrarily close to \( \gamma_0 = 0.6779 \).

**Proof.** Take \( m = 3r + 1 \) and \( w = 3rp \) for \( p \in (1/6, 1/3) \). In the large \( r \) limit, \( \gamma \) converges to \( 3(1 - S(p)/S(3p)) \) where \( S(p) = -p \log_2 p - (1 - p) \log_2 p \), which can be seen by the Stirling approximation. At \( p = 0.270629 \), we have \( \gamma = 0.6779 \). \( \square \)

We have verified that the smallest code such that \( m = 3r + 1 \) with \( \gamma < 1 \) has \( r = 19 \) and \( w = 14 \) so the code is \([288215893050995568, 14483100716176, 21700] \).

### III. DISCUSSION

We have given a code with \( \gamma < 1 \). It is not clear what the infimum of \( \gamma \) over all codes is; indeed, we know no proof that \( \gamma \) is bounded away from zero. The \( r = 19, w = 14 \) is quite large, but Ref. [6] used random puncturing of Reed-Muller codes followed by removing certain punctures to increase distance to find codes with less than 1000 qubits and \( \gamma < 1.2 \), giving reason to hope that future work may find smaller examples with \( \gamma < 1 \).

One may also ask for the infimum of \( \gamma \) over codes with \( k = 1 \). We do not know any such code with \( \gamma < 2 \) (the random triorthogonal codes of Ref. [6] and the protocols of Ref. [5] both allow \( \gamma \rightarrow 2 \) for \( k = 1 \)).

---

[1] Sergey Bravyi and Jeongwan Haah, “Magic-state distillation with low overhead,” Physical Review A 86, 052329 (2012).

[2] E. Knill, “Fault-tolerant postselected quantum computation: Schemes,” (2004). quant-ph/0402171v1

[3] Sergey Bravyi and Alexei Kitaev, “Universal quantum computation with ideal Clifford gates and noisy ancillas,” Phys. Rev. A 71, 022316 (2005) quant-ph/0403025.

[4] Cody Jones, “Multilevel distillation of magic states for quantum computing,” Phys. Rev. A 87, 042305 (2013).

[5] Jeongwan Haah, Matthew B. Hastings, D. Poulin, and D. Wecker, “Magic state distillation with low space overhead and optimal asymptotic input count,” 1703.07847v1

[6] Jeongwan Haah and Matthew B. Hastings, (2017).

[7] Harold N. Ward, “Weight polarization and divisibility,” Discrete Mathematics 83, 315–326 (1990).

[8] F. J. MacWilliams and N. J. A. Sloane, The Theory of Error-Correcting Codes (North-Holland, 1977).