Short $\text{QMA}(k)$ Proofs for SAT without Entangling Measurements

Jing Chen and Andrew Drucker

December 17, 2008

Abstract

$\text{BellQMA}(k)$ is the subclass of $\text{QMA}(k)$ in which the verifier is restricted to perform unentangling measurements on the proofs received from each Merlin. $\text{BellQMA}_{O(\log m)}(\tilde{O}(\sqrt{m}))$ is the class of promise problems having $\text{BellQMA}$ proofs with $\tilde{O}(\sqrt{m})$ provers, each sending an $O(\log m)$-qubit message, and with a constant completeness-soundness gap. In this paper, we prove that a $3\text{SAT}$ instance with $m$ clauses has a $\text{BellQMA}_{O(\log m)}(\tilde{O}(\sqrt{m}))$ proof of satisfiability. Our result improves the result of Aaronson, Beigi, Drucker, Fefferman, and Shor in [ABDFS’08], who showed that $3\text{SAT}$ has a $\text{QMA}_{O(\log m)}(\tilde{O}(\sqrt{m}))$ proof with a constant completeness-soundness gap.

1 Introduction

In Quantum Merlin-Arthur proof systems, a computationally unbounded but untrusted prover Merlin tries to convince a polynomial-time quantum verifier Arthur that a given statement is true, by sending to Arthur a polynomial-size quantum state as a ‘proof’. We desire that the protocol have two properties. The first is ‘completeness’: if the statement is true, then there should exist a proof which makes Arthur accept with high probability, say at least $2/3$. The second is ‘soundness’: if the statement is false, then for any proof received, Arthur should accept with probability at most $1/3$. The complexity class $\text{QMA}$ consists of all languages $L$ whose membership can be proved by a $\text{QMA}$ proof system.

The generalized multi-prover version of $\text{QMA}$, $\text{QMA}(k)$ ($k \geq 2$), was introduced by Kobayashi, Matsumoto, and Yamakami in [KMY’03]. In a $\text{QMA}(k)$ proof system, $k$ Merlins are trying to convince a single Arthur that a given statement is true, by each sending Arthur a quantum proof, and these $k$ proofs are assumed to be unentangled with each other. Again we seek completeness $2/3$ and soundness $1/3$.

One piece of evidence for the additional power of multiple provers came from Aaronson et al [ABDFS’08], who showed that if $k$ is allowed to scale as $\tilde{O}(\sqrt{m})$, Arthur can be convinced of the satisfiability of an $m$-clause $3\text{SAT}$ instance by $k$ proofs of $O(\log m)$ qubits each. This gives an almost-quadratic improvement in proof length compared to classical proofs for $n$-variable instances (when $m = O(n)$). A related but incomparable result was given in [BT’08], where it was shown that 2 provers with proofs of length $O(\log n)$ can prove 3-colorability of $n$-vertex graphs, if the completeness-soundness gap is allowed to be only inverse-polynomial in $n$.

Despite such findings, most of the important questions about $\text{QMA}(k)$ remain unanswered. In particular, it is unknown that whether the success probability of a $\text{QMA}(k)$ proof can be amplified by parallel repetition. This is because, by performing a joint (entangling) measurement on the proof states provided by the provers for one trial, Arthur may cause the proofs provided by these provers for the next trial to become entangled, thus destroying the conditions which guaranteed the original protocol’s soundness.

This observation makes it natural to wonder about the power of $\text{QMA}(k)$ protocols in which Arthur only performs unitary transformations and measurements whose action is local to a single prover’s register, as soundness amplification of such protocols presents no difficulties. [ABDFS’08] defined the class $\text{BellQMA}(k)$ as the set of languages for which such a restricted $\text{QMA}(k)$ protocol may be given, and asked about the computational power of these protocols. Brandao [B’08] subsequently showed $\text{BellQMA}(k) = \text{QMA}$ for any
constant $k$, suggesting their power is limited. However, Brandao’s approach does not seem to apply to values of $k$ which are allowed to grow with $n$, leaving hope that for such $k$ novel protocols might emerge.

We show this is the case, by exhibiting a multi-prover BellQMA($k$) protocol for 3SAT that essentially matches the parameters of the QMA($k$) protocol from [ABDFS’08] (we do, however, lose perfect completeness). Our techniques are a combination of those found in [ABDFS’08] and [BT’08]. We follow [ABDFS’08] in our use of size-efficient PCP reductions to improve soundness, and in the way we exploit the ‘birthday paradox’, but we borrow the Fourier tests used in [BT’08], using them in a novel fashion to avoid the entangling swap-test measurements common to both papers. Our main theorem, to which the paper will be devoted, is the following:

**Theorem 1.** There is a BellQMA protocol which, given a 3SAT instance with $m$ clauses, uses $\tilde{O}(\sqrt{m})$ Merlins, each of which sends $O(\log m)$ qubits. The protocol is polynomial-time and has completeness $1 - \exp\{-\Omega(\sqrt{m})\}$ and soundness $1 - \Omega(1)$.

## 2 2-CSPs with Constant Soundness Gap.

Say Arthur is given a Boolean formula $\varphi(x)$ of size $m$ (that is, $\varphi(x)$ has $m$ clauses) which he wishes to be convinced is satisfiable. The recent version of the PCP Theorem given by Dinur [D’07] provides a reduction from the question of formula satisfiability to a problem called constraint graph, or 2-CSP. A constraint graph is an undirected graph (possibly with self-loops) with $n$ vertices. There is associated to the graph a set $\Sigma$ of “colors” such that $|\Sigma| = K = O(1)$. For each edge $e = (u, v) \in E$ the constraint graph has an associated binary relation $R_e : \Sigma \times \Sigma \rightarrow \{0, 1\}$. A coloring $\tau : V \rightarrow \Sigma$ satisfies the constraint $R_e$ if $R_e(\tau(u), \tau(v)) = 1$. We say that $G$ is satisfiable if there exists a mapping $\tau$ that satisfies all constraints. We say that $G$ is $(1 - \eta)$-unsatisfiable if for all mappings $\tau : V \rightarrow \Sigma$, the fraction of constraints satisfied by $\tau$ is at most $(1 - \eta)$.

**Theorem 2.** ([D’07]) There exists a reduction $T$ from SAT instances to 2-CSP instances, with the following properties:

1. (Completeness) If $\varphi$ is a satisfiable formula, $T(\varphi)$ is a satisfiable 2-CSP instance;
2. (Soundness) There exists an absolute constant $\eta > 0$ such that if $\varphi$ is unsatisfiable, $G = T(\varphi)$ is $(1 - \eta)$-unsatisfiable;
3. (Size-Efficiency) If $|\varphi| = m$, $|V(G)| = n = O(m \cdot \text{polylog } m)$;
4. (Alphabet Size) $|\Sigma| = K = O(1)$;
5. (Regularity) $G$ is $d$-regular (with self-loops), $d = O(1)$.

The last point is not quite explicit in the main statement of Dinur’s result, but can be readily extracted from her proof: simply apply her ‘Preprocessing Transformation’ of Lemma 7 to the graph output by her main reduction. Also, Dinur’s reduction takes as input a constraint graph, not a formula, but we can simply begin by transforming any SAT instance of size $m$ into an equivalent instance of an NP-hard 2-CSP such as 3-Colorability, yielding a constraint graph whose number of vertices is $O(m)$.

In our protocol, Arthur and Merlins first run the above reduction, yielding a 2-CSP $G$ on $n = \tilde{O}(m)$ vertices that is either satisfiable or $(1 - \eta)$-unsatisfiable. We now describe our BellQMA protocol for the problem, starting directly from $G$, with $O(\sqrt{n}) = \tilde{O}(\sqrt{m})$ unentangled proofs, each proof consisting of $O(\log n) = O(\log m)$ qubits.

## 3 Our Protocol

Given a graph $G$, let the proofs be $|\Psi_1\rangle, \ldots, |\Psi_{C\sqrt{n}}\rangle$, with $C$ a constant (to be assigned). Each $|\Psi_i\rangle$ consists of a node register with base states $|0\rangle, \ldots, |n-1\rangle$ ($\log n$ qubits) and a color register with base states $|0\rangle, \ldots, |K-1\rangle$ ($\log K$ qubits). Let $\mu \triangleq \frac{C\sqrt{n}}{K}$. The verifier’s protocol is given below.
Verifier $V$

- Flip a fair coin. If Heads, do the Uniform Test; if Tails, do the Consistency Test.
- Uniform Test:
  1. For each $|\Psi_i\rangle$, perform a Fourier transform $F_K$ on the color register and measure it. Let $Z = \{i : |\Psi_i\rangle$ is measured 0\}. If $|Z| \not\in [\frac{99\mu}{100}, \frac{101\mu}{100}]$, reject; otherwise continue.
  2. For each $|\Psi_i\rangle$ such that the measurement in Step 1 gets 0, perform a Fourier transform $F_n$ on the node register and measure it. If there exits a $|\Psi_i\rangle$ such that the measurement doesn’t get 0, reject; otherwise accept.
- Consistency Test:
  1. For each $|\Psi_i\rangle$, measure it and denote the value in the two registers as $(v_i, c_i)$.
  2. If there exists two states $|\Psi_i\rangle$ and $|\Psi_j\rangle$ such that $e = (v_i, v_j) \in E$ but $R_e(c_i, c_j) = 0$, reject; also reject if $v_i = v_j$ but $c_i \neq c_j$. Otherwise, accept.

3.1 Completeness of Our Protocol

From now on, we use $\hat{i}$ to denote the square root of $-1$, while reserve the symbol $i$ for the index of the proofs sent by Merlins.

**Theorem 3.** If $G$ is satisfiable, then there exists unentangled $|\Psi_1\rangle, \ldots, |\Psi_{C\sqrt{n}}\rangle$ such that $V$ accepts with probability at least $1 - \exp\{-\frac{\mu}{2 \cdot 10^4}\} = 1 - \exp\{-\Omega(\sqrt{n})\}$.

**Proof.** Let $|\Psi_i\rangle = |\Psi\rangle \triangleq \frac{1}{\sqrt{n}} \sum_{v=0}^{n-1} |v\rangle |\tau(v)\rangle$ for all $i \leq C\sqrt{n}$, where $\tau$ is a valid mapping for the graph $G$.

Since $\tau$ is valid, we have that the Consistency Test will accept with probability 1.

Notice that a Fourier transform on the color register will change $|\Psi\rangle$ into

$$(I_n \otimes F_K) \frac{1}{\sqrt{n}} \sum_{v=0}^{n-1} |v\rangle |\tau(v)\rangle = \frac{1}{\sqrt{n}} \sum_{v=0}^{n-1} |v\rangle \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} \exp\{-\frac{2\pi i \tau(v)k}{K}\} |k\rangle.$$  

(1)

Thus for each $|\Psi_i\rangle$, the measurement in Step 1 of the Uniform Test will get 0 with probability $n \cdot (\frac{1}{\sqrt{n}})^2 \cdot (\frac{1}{\sqrt{K}})^2 = \frac{1}{K}$. Therefore $E[|Z|] = \frac{C\sqrt{n}}{K} = \mu$. Since $|\Psi_i\rangle$’s are unentangled, they will be measured 0 independently. According to Chernoff Inequality, we have that

$$\Pr \left[ |Z| \in \left[ \frac{99\mu}{100}, \frac{101\mu}{100} \right] \right] = 1 - \Pr \left[ |Z| \not\in \left[ \frac{99\mu}{100}, \frac{101\mu}{100} \right] \right] = 1 - 2 \exp\{-\frac{\mu}{2 \cdot 10^2}\}.$$  

Further notice that according to Equation (1), given that the color register is measured 0, the state in the node register of $|\Psi\rangle$ becomes $\frac{1}{\sqrt{n}} \sum_{v=0}^{n-1} |v\rangle$, and a Fourier transform $F_n$ will change this state into

$$F_n \frac{1}{\sqrt{n}} \sum_{v=0}^{n-1} |v\rangle = \frac{1}{\sqrt{n}} \sum_{v=0}^{n-1} \frac{1}{\sqrt{n}} \sum_{u=0}^{n-1} \exp\{\frac{2\pi i vu}{n}\} |u\rangle = |0\rangle.$$  

Thus for each $|\Psi_i\rangle$ which is measured 0 in Step 1 of the Uniform Test, Step 2 of this test will measure it to 0 with probability 1.

Thus the probability that $V$ accepts is at least

$$\frac{1}{2} \cdot (1 - 2 \exp\{-\frac{\mu}{2 \cdot 10^2}\}) \cdot 1 + \frac{1}{2} \cdot 1 = 1 - \exp\{-\frac{\mu}{2 \cdot 10^1}\}.$$  

$\square$
4 Soundness of Our Protocol

Now consider the case when $G$ is not satisfiable. We have the following theorem:

**Theorem 4.** If $G$ is not satisfiable, then for all proofs $(|Ψ_1⟩, \ldots, |Ψ_{C,\sqrt{m}}⟩)$, $V$ will reject with probability $Ω(1)$.

The proof of this theorem depends on a sequence of lemmas.

For each $i ∈ [C, \sqrt{m}]$, let $|Ψ_i⟩ = \sum_{v=0}^{n-1} α_i^v |v⟩ \sum_{j=0}^{K-1} β_{v,j}^i |j⟩$, where $\sum_{v=0}^{n-1} |α_i^v|^2 = 1$ and $\sum_{j=0}^{K-1} |β_{v,j}^i|^2 = 1$ for each $i$ and each $v$. Let $p^i_0$ be the probability that $|Ψ_i⟩$ is measured 0 in Step 1 of the Uniform Test. Let $Z' = \{i : p^i_0 ≥ \frac{1}{2K}\}$, $P^i_{U_1}$ the probability that $V$ rejects in Step 1 of the Uniform Test, $P^i_{U_2}$ the probability that $V$ rejects in Step 2 of the Uniform Test, and $P^r$ the probability that $V$ rejects (taking into account the random coin of $V$). We have the following lemma.

**Lemma 1.** If $|Z'| ≤ \frac{µ}{2}$, then $P^r > 1 - \exp\{-\frac{24^2 µ}{1252.8\cdot 3}\} = Ω(1)$.

**Proof.** Let $Z_1 = Z \cap Z'$ and $Z_2 = Z \cap ([C, \sqrt{m}] \setminus Z')$, we have that $|Z| = |Z_1| + |Z_2|$, $|Z_1| ≤ |Z'| ≤ \frac{µ}{2}$, and $Pr[i \in Z_2] < \frac{1}{2K} \forall i \in [C, \sqrt{m}]$. Let $Z_3$ be a random subset of $[C, \sqrt{m}]$ such that $Pr[i \in Z_3] = \frac{1}{2K}$ independently for every $i$, we have that $E[|Z_3|] = \frac{C, \sqrt{m}}{2K} = \frac{µ}{2}$.

By Chernoff’s bound, we have that the probability that $V$ passes Step 1 of the Uniform Test is

$$ P^i_{U_1} = Pr[|Z| ≥ \frac{99µ}{100}] ≤ Pr[|Z| ≥ \frac{99µ}{100}] = Pr[|Z_1| + |Z_2| ≥ \frac{µ}{2} + \frac{24µ}{100}] $$

$$ ≤ Pr[|Z_2| ≥ \frac{µ}{4} + \frac{24µ}{100}] < Pr[|Z| ≥ \frac{µ}{4} + \frac{24µ}{100}] $$

$$ < \exp\{-\frac{24^2 µ}{1252.8\cdot 3}\} < \exp\{-\frac{24^2 µ}{1252.8}\}. $$

Thus $P^i_{U_1} = 1 - P^i_{U_1} > 1 - \exp\{-\frac{24^2 µ}{1252.8}\}$, and $P^r ≥ \frac{P^r_{U_1}}{2}$ as desired. 

According to Lemma 1, we just need to consider the case of $|Ψ_i⟩$’s such that $|Z'| > \frac{µ}{2}$. Let $ε < \frac{µ}{20}$ be a constant, where $η$ is the soundness constant in Dinur’s PCP reduction, and let $R_i = \{v : v ∈ V, |α_i^v|^2 < \frac{1}{8Kn}\}$ for each $i ∈ [C, \sqrt{m}]$. We have the following lemma.

**Lemma 2.** If there exists $i ∈ Z'$ such that $|R_i| ≥ εn$, then $P^r ≥ \frac{ε^2}{125K} = Ω(1)$.

**Proof.** After the Fourier transform in Step 1 of the Uniform Test, $|Ψ_1⟩$ becomes

$$ (I_n ⊗ F_K) \sum_{v=0}^{n-1} α_i^v |v⟩ \sum_{j=0}^{K-1} β_{v,j}^i |j⟩ = \sum_{v=0}^{n-1} α_i^v |v⟩ \sum_{j=0}^{K-1} β_{v,j}^i \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} \exp\{\frac{2πijk}{K}\} |k⟩ \tag{2} $$

$$ = \frac{1}{\sqrt{K}} \sum_{k=0}^{K-1} \left( \sum_{v=0}^{n-1} α_i^v \sum_{j=0}^{K-1} β_{v,j}^i \exp\{\frac{2πijk}{K}\} \right) |v⟩ |k⟩. \tag{3} $$

Let $X = \sum_{v=0}^{n-1}γ_i^v |v⟩$ be the state left in the node register when the color register is measured 0. By Equation (3) we have that for each $v$,

$$ γ_i^v = \frac{1}{\sqrt{K}} α_i^v \sum_{j=0}^{K-1} β_{v,j}^i \exp\{\frac{2πijk}{K}\}. $$
By Equation (2) we have that for each $v$, conditioned on the node register being state $|v\rangle$, the probability that the color register is measured 0 is exactly $\frac{1}{\pi} |\sum_{j=0}^{K-1} \beta_{v,j}|^2 \leq 1$. Moreover, since $i \in Z'$, $p_i^0 = \frac{1}{K} \sum_{v=0}^{n-1} |\alpha_v^i| \sum_{j=0}^{K-1} \beta_{v,j}^i|^2 \geq \frac{1}{4K}$. Therefore for all $v$, we have that

$$|\gamma_v^i|^2 \leq 4K |\alpha_v^i|^2 (\frac{1}{K} \sum_{j=0}^{K-1} \beta_{v,j}^i|^2) \leq 4K |\alpha_v^i|^2.$$

Accordingly, for each $v \in R_i$, $|\gamma_v^i|^2 \leq \frac{4K}{8K^n} = \frac{1}{2^n}$.

Let $p_i^r$ be the probability that $|\Psi_i\rangle$'s node register isn't measured to 0 in Step 2 of the Uniform Test given that its color register is measured 0 in Step 1 (therefore $\mathcal{V}$ rejects). Adopting the same idea in the proof of Lemma 2.12 of [BT’08], we have that

$$p_i^r = 1 - |\langle X|0\rangle|^2 \geq \left(\frac{1}{2} \sum_{v=0}^{n-1} |\gamma_v|^2 - \frac{1}{n}\right)^2 \geq \frac{1}{4} \left(\sum_{v \in R_i} |\gamma_v|^2 - \frac{1}{n}\right)^2 \geq \frac{1}{4} \left(\frac{\epsilon n}{2n}\right)^2 = \frac{\epsilon^2}{16}.$$

Because the probability that $\mathcal{V}$ rejects in Step 2 of the Uniform Test is at least $p_i^r$ given that $|\Psi_i\rangle$'s color register is measured 0 in Step 1, we have that the probability that $\mathcal{V}$ rejects in Step 2 of the Uniform Test (without conditioned on anything) is

$$P_{U_2}^r \geq p_i^0 \cdot p_i^r \geq \frac{1}{4K} \cdot \frac{\epsilon^2}{16} = \frac{\epsilon^2}{64K},$$

and thus $P_r \geq \frac{P_{U_2}^r}{2} \geq \frac{\epsilon^2}{128K}$, as desired.

According to Lemma 2, now we just need to consider the case when $|Z'| > \frac{\mu}{2}$ and $|R_i| < \epsilon n \forall i \in Z'$. We show that in this case the Consistency Test rejects with probability $\Omega(1)$. Restrict attention to $i \in Z'$.

Let $D_i$ denote the distribution on vertex/color pairs when $|\Psi_i\rangle$ is measured by the Consistency Test. We can generate each $D_i$ as $D_i = g_i(U_i)$, where each $U_i$ is a uniformly, independently drawn real from $[0,1]$ and $g_i : [0,1] \rightarrow V(G) \times \Sigma$ is a function such that each preimage $g_i^{-1}((v,c))$ is an interval of length equal to $\Pr[D_i = (v,c)]$.

Clearly we can arrange these preimages so that $g_i^{-1}(v,\ast)$ forms an interval for each $v$. For each $v \notin R_i$, $g_i^{-1}(v,\ast)$ is of length at least $\frac{1}{8K^n}$; select a subinterval $J_{i,v}$ of length exactly $\frac{1}{8K^n}$. Let $J_i = \bigcup_{v \notin R_i} J_{i,v}$. Observe the following: first, $J_i$ has measure greater than $\frac{(1-\epsilon^2)}{8K^n}$. Second, for any $i \in Z'$, if we condition on the event $U_i \in J_i$, the posterior distribution of the vertex $v_i$ outputted by $D_i$ is now uniform over $S_i \triangleq [n] \setminus R_i$.

So in our analysis of the Consistency Test (applied to a fixed collection of proofs $Z'$ satisfying $|Z'| > \frac{\mu}{2}$ and $|R_i| < \epsilon n \forall i \in Z'$), let us generate all measurements on $Z'$ by this scheme, and condition first on which proofs $|\Psi_i\rangle$ in $Z'$ satisfy $U_i \in J_i$ (let $Z''$ denote this random collection). Notice that $E[|Z''|] > \frac{(1-\epsilon)\mu}{16K} > \frac{(1-\epsilon)2\sqrt{\pi}}{16K}$, and $|Z''|$ is never greater than $C\sqrt{n}$. Let $p$ denote the probability that $|Z''| > \frac{(1-\epsilon)\mu}{16K}$, where $p \geq \frac{E[|Z''|]}{2(C\sqrt{n} - E[|Z''|]/2)} \geq \frac{(1-\epsilon)}{32K^2} = \Omega(1)$.

Thus with $\Omega(1)$ probability $|Z''| \geq m' := \frac{(1-\epsilon)2\sqrt{\pi}}{32K^2}$. The following Lemma tells us that if $C$ is chosen as a suitably large constant, then conditioned on $|Z''| \geq m'$, the Consistency Test rejects with high probability.
Lemma 3. Let \((G, \{R_e\})\) be a \(d\)-regular constraint graph (possibly with self-loops, and \(d > 1\)) with alphabet \(K\). Say \(G\) is \((1 - \eta)\)-unsatisfiable. Let \(D_1, \ldots, D_{n'}\) be independent distributions on \(V(G) \times \Sigma\), with \((v_i, c_i)\) denoting the output of \(D_i\). Suppose for each \(i \leq n'\) there exists an \(S_i \subseteq V(G)\) of size at least \((1 - \epsilon)n\), such that \(v_i\) is uniformly distributed over \(S_i\). Then we can set \(n' = O(\sqrt{n})\) large enough that with probability at least .99 there exists \(i < j \leq n'\) such that either \(e = (v_i, v_j)\) is an edge of \(G\) and \(R_{e}(c_i, c_j) = 0\), or \(v_i = v_j, c_i \neq c_j\).

Remark: The constant in the \(O()\) notation depends on \(d, \epsilon\) and \(\eta\), but not \(K\). In our application of this Lemma, we let \(D_1, \ldots, D_{n'}\) be the residual distributions on the set of proofs in \(Z''\), after conditioning on their membership in \(Z''\).

Proof. For \(i < j \leq n'\), let \(V_{i,j}\) be the indicator (0/1) random variable for the event that either \(e = (v_i, v_j) \in E(G)\) and \(R_{e}(c_i, c_j) = 0\), or \(v_i = v_j\) and \(c_i \neq c_j\). Let \(V = \sum_{i<j} V_{i,j}\). To prove the Lemma it is enough to show that \(\Pr[V = 0] \leq .01\). We show this using the second moment method.

A first observation is that we can have each \(D_i\) be generated in the following way: first randomly select a coloring \(\tau_i\) according to some distribution \(L_i\); next select \(v_i\) uniformly from \(S_i\), and set \(c_i = \tau_i(v_i)\). To be explicit, each \(L_i\) independently chooses colors according to the rule \(\Pr[\tau_i(v) = c] = \Pr[c_i = c|v_i = v]\). It is easily verified (by reversing the order of the two independent steps) that this process yields \(D_i\). The perspective of choosing the colorings \(\tau_i\) first will be useful to us in what follows.

Next we lower-bound \(\E[V] = \sum_{i<j} \E[V_{i,j}]\). Fix any \(i < j \leq n'\). Condition on any choice of the colorings \(\tau_i, \tau_j\); we will show that \(\E[V_{i,j} | \tau_i, \tau_j] \geq \frac{\eta}{n}\). Let \(P_{i,j} \subseteq V(G)\) be the subset of vertices \(v\) for which \(\tau_i(v) = \tau_j(v)\). Suppose first that \(|P_{i,j}| \leq (1 - 3\epsilon)n\). In this case there are at least \(en\) vertices contained in \(S_i \cap S_j \cap \overline{P_{i,j}}\), and \(V_{i,j} = 1\) whenever a vertex in this set is selected as both \(v_i\) and \(v_j\). Thus in this case \(\E[V_{i,j} | \tau_i, \tau_j] \geq e\cdot \frac{1}{|S_i|} \cdot \frac{1}{|S_j|} \geq \frac{\eta}{n}\).

For our second case, suppose \(|P_{i,j}| > (1 - 3\epsilon)n\). Consider the induced subgraph \(G[S_i \cap S_j \cap P_{i,j}]\), which contains at least \(n - 2en - 3en = (1 - 5\epsilon)n\) vertices. Since \(G\) has maximum degree \(d\), \(|E(G)| = \frac{dn}{2}\), and the set \(\overline{S_i} \cup \overline{S_j} \cup \overline{P_{i,j}}\) is incident on at most \(d(5en)\) edges, we have that \(|E(G[S_i \cap S_j \cap P_{i,j}])| \geq \frac{dn}{2} - 5den = (1 - 10\epsilon)\frac{dn}{2} = (1 - 10\epsilon)|E(G)|\). By \((1 - \eta)\)-unsatisfiability of \((G, \{R_e\})\), \(\tau_i\) satisfies less than a \(\frac{1}{1-10\epsilon}\) fraction of the edge constraints in \(G[S_i \cap S_j \cap P_{i,j}]\). Thus the fraction of these constraints which are violated by \(\tau_i\) is more than \(1 - \frac{1-\eta}{1-10\epsilon} = \frac{1-10\epsilon(1-\eta)}{1-10\epsilon} > \frac{2\eta}{\frac{1}{2} - 10\epsilon} > \frac{\eta}{2},\) since \(\eta > 20\epsilon\).

Now \(\tau_j \equiv \tau_i\) on \(P_{i,j}\). We can thus lower-bound \(\E[V_{i,j} | \tau_i, \tau_j]\) by the probability that \(v_i, v_j \in S_i \cap S_j \cap P_{i,j}\) and form (in either order) an edge violated by the color assignment \((\tau_i(v_i), \tau_j(v_j))\). Note that some edges are self-loops and so may only be chosen in one way. We get

\[
\E[V_{i,j} | \tau_i, \tau_j] \geq (1 - 5\epsilon)^2 \cdot \frac{\eta}{2} (1 - 10\epsilon)|E(G)|\frac{|E(G[S_i \cap S_j \cap P_{i,j}])|}{n^2} = \frac{\eta (1 - 5\epsilon)^2 (1 - 10\epsilon)d}{4n}.
\]

Recall that \(\epsilon < \frac{\eta}{20} < \frac{1}{20},\) so the quantity above is greater than \(\frac{2^{2-3d}}{4n} > \frac{n}{20m} > \frac{\eta}{n}\), as needed (using \(d > 1\)). Thus in either of our two cases we conclude \(\E[V_{i,j} | \tau_i, \tau_j] \geq \frac{\eta}{n}\), so \(\E[V_{i,j}] \geq \frac{\eta}{n}\) unconditioned as well. Summing over all \(i < j\), we find \(\E[V] \geq \frac{\eta}{n}\).

Next we upper-bound \(\E[V^2] = \sum_{i<j,k<l} \E[V_{i,j}V_{k,l}]\). There are \(\binom{n'}{2}\) terms for which \((i,j) = (k,l)\). For each such term \(\E[V_{i,j}^2] = \E[V_{i,j}]\). Condition on the vertex \(v_i\) outputted by \(D_i\). Fixing any such choice of \(v_i\), the probability that \(V_{i,j} = 1\) is of course upper-bounded by the probability that \(v_j\) is equal or adjacent to \(v_i\) in \(G\). Since \(v_j\) is uniform on \(S_i\) and \(v_i\) is of degree \(d\), this probability is at most \(\frac{d+1}{|S_i|} \leq \frac{d+1}{(1-\epsilon)n}\), so \(\E[V_{i,j} | v_i] \leq \frac{d+1}{(1-\epsilon)n}\). As \(v_i\) was an arbitrary conditioning we conclude \(\E[V_{i,j}] \leq \frac{d+1}{(1-\epsilon)n}\). Thus the contribution to \(\E[V^2]\) from these terms is at most \(\binom{n'}{2}(d+1)(1-\epsilon)n\).
If \((i,j), (k,l)\) consists of three distinct indices, assume that \(j = l\) (the other cases are handled similarly). Condition on any choice of \(v_j\). Then \(V_{i,j}V_{j,k} = 1\) can only occur if \(v_j\) and \(v_k\) are each either adjacent or equal to \(v_j\). These two events are independent after conditioning on \(v_j\) since \(D_i, D_j, D_k\) are independent. Thus $$\mathbb{E}[V_{i,j}V_{j,k}] \leq \left( \frac{d+1}{(1-\epsilon)n} \right)^2.$$ 

For any three distinct indices \(a < b < c \leq m'\), there are six tuples \((i < j), (k < l)\) for which \(\{i, j, k, l\} = \{a, b, c\}\). In each case the above analysis applies (with trivial modifications). Thus the contribution to \(\mathbb{E}[V^2]\) from these ‘triplet’ terms is at most $$6\left( \frac{(m')^3(d+1)^2}{(1-\epsilon)n^2} \right) \leq \left( \frac{(m')^3(d+1)^2}{(1-\epsilon)n^2} \right).$$ 

If \((i, j), (k, l)\) are four distinct elements of \([m']\), then the pair \(V_{i,j}, V_{j,k}\) depend on disjoint sets of independent random variables, so that \(\mathbb{E}[V_{i,j}V_{j,k}] = \mathbb{E}[V_{i,j}]\mathbb{E}[V_{j,k}]\). Thus the contribution to \(\mathbb{E}[V^2]\) from these terms is upper-bounded by $$\sum_{(i<j), (k<l)} \mathbb{E}[V_{i,j}]\mathbb{E}[V_{j,k}] = \mathbb{E}[V]^2.$$ 

Putting things together, $$\mathbb{E}[V^2] < \left( \frac{m'}{2} \right)\left( \frac{d+1}{1-\epsilon} \right) + \frac{(m')^3(d+1)^2}{(1-\epsilon)^2n^2} + \mathbb{E}[V]^2.$$ 

With this bound in hand, we apply Chebyshev’s inequality:

$$\Pr[V = 0] \leq \Pr[|V - \mathbb{E}[V]| \geq \mathbb{E}[V]] \leq \frac{\mathbb{E}[V^2] - \mathbb{E}[V]^2}{\mathbb{E}[V]^2} \leq \frac{\left( \frac{m'}{2} \right)\left( \frac{d+1}{1-\epsilon} \right) + \frac{(m')^3(d+1)^2}{(1-\epsilon)^2n^2}}{\mathbb{E}[V]^2} = O\left( \frac{n}{(m')^2} + \frac{1}{m'} \right),$$

where we suppress dependence on the constants \(\epsilon, d\). Thus by taking \(m'\) a suitably large value in \(O(\sqrt{n})\), we find that \(V = 0\) with probability at most .01. This proves the Lemma.

Applying this Lemma, we find that whenever \(|Z'| > \frac{\mu}{2}\) and \(|R_i| < \epsilon n\ \forall i \in Z'\), the Consistency Test rejects with probability \(\Omega(1)\). Showing soundness in this final case completes the proof that our protocol possesses soundness \(\Omega(1)\).

\[\square\]

5 Acknowledgements

We want to thank Scott Aaronson for his great lectures and suggestions.

References


