Electronic Colloquium on Computational Complexity, Report No. 37 (2026)

A Note on the Equivalence Between Zero-knowledge and Quantum CSS Codes

Noga Ron-Zewi[*] Mor Weiss [†]

Abstract

Zero-knowledge codes, introduced by Decatur, Goldreich, and Ron [DGR20], are error-correcting codes in which few codeword symbols reveal no information about the encoded message, and have been extensively used in cryptographic constructions. Quantum CSS codes, introduced by Calderbank and Shor [CS96] and Steane [Ste96], are error-correcting codes that allow for quantum error correction, and are also useful for applications in quantum complexity theory. In this short note, we show that (linear, perfect) zero-knowledge codes and quantum CSS codes are equivalent. We demonstrate the potential of this equivalence by using it to obtain explicit asymptotically-good zero-knowledge locally-testable codes.

1 Introduction

In this note, we show an equivalence between two well-studied families of codes: Zero-knowledge codes and quantum CSS codes. We first briefly describe these families of codes and their applications.

Zero-knowledge codes. Zero-Knowledge (ZK) codes are error-correcting codes with a randomized encoding, in which few codeword symbols reveal nothing about the encoded message. More accurately, a *t-Zero-Knowledge* (ZK) code $C \subseteq \mathbb{F}^n$, for some $t \in \mathbb{N}$, is associated with a randomized encoding map $\mathsf{Enc}_C : \mathbb{F}^k \to \mathbb{F}^n$ and has the following guarantee. For every $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^k$, and any $\mathcal{I} \subseteq [n]$ of size $|\mathcal{I}| \leq t$, we have that $\mathsf{Enc}_C(\mathsf{m})|_{\mathcal{I}}$ and $\mathsf{Enc}_C(\mathsf{m}')|_{\mathcal{I}}$ are identically distributed, where $\mathsf{Enc}_C(\mathsf{m})|_{\mathcal{I}}$ denotes the restriction to $\mathcal{I}$ of a randomly-generated encoding of m. In this note, we focus on *non-adaptive, perfect* ZK codes, as defined above. That is, the queries of an adversary to the codeword are determined non-adaptively, and the resultant distribution is identical for every pair of messages. We note that the non-adaptive and adaptive settings are known to be equivalent [BCL22, Appendix C], and that relaxations to the statistical setting (where the distributions $\mathsf{Enc}_C(\mathsf{m})|_{\mathcal{I}}, \mathsf{Enc}_C(\mathsf{m}')|_{\mathcal{I}}$ are statistically close) have also been considered in the literature [ISVW13]. We additionally focus on *linear* ZK codes, meaning that C is a linear subspace of $\mathbb{F}^n$, and the encoding map Enc_C is linear in the message m and the randomness used for encoding.

ZK codes were first formally defined by Decatur, Goldreich, and Ron [DGR20], and have been used (either explicitly or implicitly) in numerous applications in cryptography. For example, these codes have been used in Shamir's secret sharing [Sha79], and lie at the heart of information-theoretically secure Multi-Party Computation (MPC) protocols (starting from [BGW88, CCD88]). ZK codes also have applications to memory delegation (e.g., in PIR schemes [CGKS95]), as well as

[*] Department of Computer Science, University of Haifa. Email: `noga@cs.haifa.ac.il`.

[†] Faculty of Engineering, Bar-Ilan University. Email: `mor.weiss@biu.ac.il`.

ISSN 1433-8092

for the design of information-theoretic proofs systems such as Probabilistically Checkable Proofs (PCPs) [ALM+92, AS92] and Interactive Oracle Proofs (IOPs) [BCS16, RRR16] with ZK guarantees (e.g., in [BCGV16, BCF+17, CFGS18, BBHR19, BCL22, RW24, GOS25]).

Many of the early applications of ZK codes relied on ZK properties of *polynomial-based* codes (in which the message is interpreted as a low-degree polynomial, and the corresponding codeword is the evaluation table of the polynomial). More recent work also studied and exploited ZK properties of other codes — such as concatenated codes [DGR20], interleaved codes [AHIV17, BCL22, CFW26], and tensor codes [ISVW13, BCL22, RW24] — with the goal of obtaining improved efficiency such as smaller alphabet size, higher rate, and faster encoding and decoding algorithms. These parameters are tightly connected to the efficiency measures of the resulting applications. Several other works have also studied more generally the parameters achievable by ZK codes [CCG+07, ISVW13, CDN15], suggested alternative characterizations of ZK codes [CCG+07, ISVW13, CDN15, BCL22], and introduced general frameworks for constructing such codes [DGR99, DGR20, FMSS04, ISVW13].

Quantum CSS codes. A quantum CSS code consists of a pair of linear codes $C_X, C_Z \subseteq \mathbb{F}^n$ so that their dual codes $C_X^\perp, C_Z^\perp$ are orthogonal to each other (that is, $\langle c, c' \rangle = 0$ for any $c \in C_X^\perp, c' \in C_Z^\perp$), with the additional guarantee that any vector in $C_X \setminus C_Z^\perp$ and any vector in $C_Z \setminus C_X^\perp$ has a large weight.

Quantum CSS codes were first introduced by Calderbank and Shor [CS96] and Steane [Ste96], and have been extensively studied since then. CSS codes are used to protect quantum computation from errors, and also have applications in quantum complexity theory. For example, the recent progress [ABN23] on the quantum PCP conjecture [AN02, AALV09] relied on recent breakthroughs on the construction of asymptotically good LDPC quantum CSS codes [PK22]. The resemblance of CSS codes to classical codes enables one to draw on the vast literature on classical error-correcting codes for their design, and by now we know of various constructions of such codes.

Equivalence between zero-knowledge and quantum CSS codes. In this note, we show that ZK codes and quantum CSS codes are equivalent. Specifically, we show a transformation from a ZK code into a quantum CSS code (and vice versa) so that the guarantee on the weight of vectors in $C_Z \setminus C_X^\perp$ in the CSS code translates into the ZK property of the ZK code, while the guarantee on the weight of vectors in $C_X \setminus C_Z^\perp$ translates into the decoding property of the ZK code (the latter is also typically required in applications); see Theorem 3.1 and Corollary 3.2 for a formal statement of this equivalence.

While we view this equivalence as interesting in its own right, it is also motivated by the hope that this connection might shed light on our understanding of these codes, or yield new ZK codes or CSS codes by combining the equivalence with existing constructions. We demonstrate this potential by describing one concrete application of the equivalence. Specifically, in Section 4, we translate recent breakthroughs on the construction of asymptotically-good locally testable quantum codes [DLV24, KP25, WLH25] into explicit asymptotically-good zero-knowledge locally-testable codes.

Finally, we also mention that another connection between quantum computation and zero-knowledge was discovered in [LRR19], who used fault-tolerance in the quantum setting to obtain leakage resilience in the classical computation setting. This gives another indication to the usefulness of exploring the connection between zero-knowledge and quantum computation.

2 Preliminaries

Let $\mathbb{F}$ be a finite field, and let $u, v \in \mathbb{F}^n$. We use $\langle u, v\rangle$ to denote the inner product between u, v, namely, $\langle u, v\rangle := \sum_{i=1}^n u_i \cdot v_i$. We also let $\Delta(u, v) := |\{i \in [n] : u_i \neq v_i\}|$, $\mathrm{wt}(u) := \Delta(u, 0)$, and for a subset $S \subseteq \mathbb{F}^n$, we let $\Delta(u, S) := \min_{s\in S} \Delta(u, s)$.

A linear (error-correcting) code is a subspace $C \subseteq \mathbb{F}^n$ over $\mathbb{F}$. We call $\mathbb{F}$ and n the alphabet and the block length of the code, respectively, and the elements of C are called codewords. The rate of C is the ratio $R := \frac{\dim(C)}{n}$, and it measures the amount of redundancy in encoding. The (Hamming) distance of C is $\Delta(C) := \min_{c\neq c'\in C} \Delta(c, c')$, which for a linear code equals $\mathrm{wt}(C) := \min_{0\neq c\in C} \mathrm{wt}(c)$. Intuitively, the minimum distance of a code measures the amount of noise tolerance of the code. Specifically, the channel might corrupt some of the entries of a transmitted codeword c during transmission and the receiver might receive a string $w \in \mathbb{F}^n$. However, if w and c differ on less than $\frac{\Delta(C)}{2}$ entries, then c can be recovered uniquely by the decoder by searching for the unique codeword in C that is closest to the received word w.

A generator matrix for a linear code $C \subseteq \mathbb{F}^n$ of dimension k is a (full-rank) matrix $G \in \mathbb{F}^{n\times k}$ so that $\mathrm{image}(G) = C$, and a parity-check matrix for C is a (full-rank) matrix $H \in \mathbb{F}^{(n-k)\times n}$ so that $\ker(H) = C$ (note that both G and H are not unique). The dual code of C is the code $C^\perp \subseteq \mathbb{F}^n$ containing all strings $c' \in \mathbb{F}^n$ satisfying that $\langle c', c\rangle = 0$ for all $c \in C$. It follows by definition that $(C^\perp)^\perp = C$, and that H is a parity-check matrix for C if and only if H^T is a generator matrix for $C^\perp$.

2.1 Zero-Knowledge (ZK) Codes

Zero-Knowledge (ZK) codes, introduced by Decatur, Goldreich, and Ron [DGR20], are codes in which few codeword symbols reveal no information about the message. For this to be possible, we need to associate the code C with a *randomized encoding map*, where C has ZK with respect to this randomized encoding. We will focus on an encoding map that is linear in the message and the randomness used for encoding (such a map was used in most prior works, e.g., [DGR20, BCL22, RW24]).

Definition 2.1 (Randomized Encoding Map). *Let $C \subseteq \mathbb{F}^n$ be a linear code of dimension k, let $G \in \mathbb{F}^{n\times k}$ be a generator matrix for C, and let $k' < k$ be a parameter. The k'-randomized encoding map for G is a random map $\mathsf{Enc} : \mathbb{F}^{k'} \to C$, which on input message $\mathsf{m} \in \mathbb{F}^{k'}$, samples a uniformly random $r \in \mathbb{F}^{k-k'}$, and outputs $G \cdot z$, where $z = (\mathsf{m}, r) \in \mathbb{F}^k$.*

The zero-knowledge property of an encoding map is defined as follows.

Definition 2.2 (Zero-Knowledge (ZK) Code). *Let $C \subseteq \mathbb{F}^n$ be a linear code of dimension k, let $G \in \mathbb{F}^{n\times k}$ be a generator matrix for C, and let $k' < k$ and $t < n$ be parameters. We say that the k'-randomized encoding map $\mathsf{Enc} : \mathbb{F}^{k'} \to C$ for G is t-Zero-Knowledge (t-ZK) if for any $\mathcal{I} \subseteq [n]$ of size t, and for any pair of messages $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$, we have $\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}} \equiv \mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}$.*

Error Correction in ZK Codes. Applications of zero-knowledge codes also typically require that one can recover the message $\mathsf{m} \in \mathbb{F}^{k'}$ from its randomized encoding. Specifically, let $C \subseteq \mathbb{F}^n$ be a linear code of dimension k, let $G \in \mathbb{F}^{n\times k}$ be a generator matrix for C, and let $k' < k$ be a parameter. We say that the k'-randomized encoding map $\mathsf{Enc} : \mathbb{F}^{k'} \to C$ for G is decodable from e errors if there is a (deterministic) algorithm D so that for every message $\mathsf{m} \in \mathbb{F}^{k'}$ and for every $y \in \mathbb{F}^n$ with $\mathrm{wt}(y) \leq e$, it holds that $\Pr[D(\mathsf{Enc}(\mathsf{m}) + y) = \mathsf{m}] = 1$ (see, e.g., [DGR20, Thm. 1]). Note that the existence of such a (not necessarily efficient) decoding algorithm D is equivalent to the property that for any pair of distinct messages $\mathsf{m} \neq \mathsf{m}' \in \mathbb{F}^{k'}$ and (not necessarily distinct) $r, r' \in \mathbb{F}^{k-k'}$, it holds that $\Delta(G \cdot z, G \cdot z') > 2e$, where $z = (\mathsf{m}, r)$ and $z' = (\mathsf{m}', r')$. Indeed, if this latter property holds, then given $w := \mathsf{Enc}(\mathsf{m}) + y$, the decoder D can find m by searching for $z \in \mathbb{F}^k$ so that $G \cdot z$ is closest to w.

2.2 Quantum CSS Codes

Quantum CSS codes, introduced by Calderbank and Shor [CS96] and Steane [Ste96], are error-correcting codes that allow for quantum error correction, and are defined as follows.

Definition 2.3 (CSS Code)**.** *A **CSS code** is a pair of linear codes $C_X, C_Z \subseteq \mathbb{F}^n$ so that the subspaces $C_X^\perp$ and $C_Z^\perp$ are orthogonal (that is, $\langle c, c' \rangle = 0$ for any $c \in C_X^\perp$ and $c' \in C_Z^\perp$). The **rate** of (C_X, C_Z) is $\frac{\dim(C_X) - \dim(C_Z^\perp)}{n} = \frac{\dim(C_Z) - \dim(C_X^\perp)}{n}$. The **distance** d_X (d_Z, respectively) is defined as the smallest weight of a vector of C_X not in $C_Z^\perp$ (C_Z not in $C_X^\perp$, respectively). The **distance** of (C_X, C_Z) is defined as $d = \min\{d_X, d_Z\}$.*

3 Zero-knowledge and Quantum CSS Codes Are Equivalent

We show that ZK and CSS codes (Definitions 2.2 and 2.3, respectively) are equivalent. Specifically, the following theorem shows how to transform ZK codes into CSS codes with similar parameters.

Theorem 3.1 (ZK Codes are CSS Codes)**.** *Let $C \subseteq \mathbb{F}^n$ be a linear code of dimension k, let $G \in \mathbb{F}^{n \times k}$ be a generator matrix for C, let $k' < k$ be a parameter, and let $\mathsf{Enc} : \mathbb{F}^{k'} \to C$ be the k'-randomized encoding map for G. Let $C_X = C$, and let $C_Z \subseteq \mathbb{F}^n$ be the subspace orthogonal to the span of the last $k - k'$ columns of G. Then the following holds:*

1. *$C_X^\perp$ and $C_Z^\perp$ are orthogonal (so (C_X, C_Z) is a CSS code).*
2. *$d_X > 2e$ if and only if Enc is decodable from e errors.*
3. *$d_Z > t$ if and only if Enc is t-ZK.*

The inverse transformation, from CSS Codes to ZK codes, follows as a corollary of Theorem 3.1:

Corollary 3.2 (CSS Codes are ZK Codes)**.** *Let $C_X, C_Z \subseteq \mathbb{F}^n$ be linear codes so that $C_X^\perp$ and $C_Z^\perp$ are orthogonal (i.e., (C_X, C_Z) is a CSS code). Let $k = \dim(C_X)$ and $k' = k - \dim(C_Z^\perp)$. Let $C = C_X$, let $G \in \mathbb{F}^{n \times k}$ be a generator matrix for C whose last $k - k'$ columns form a basis for $C_Z^\perp$,[1], and let $\mathsf{Enc} : \mathbb{F}^{k'} \to C$ be the k'-randomized encoding map for G. Then the following holds:*

1. *$d_X > 2e$ if and only if Enc is decodable from e errors.*
2. *$d_Z > t$ if and only if Enc is t-ZK.*

The above Corollary 3.2 follows from Theorem 3.1 by noting that $C_Z^\perp$ is exactly the span of the last $k - k'$ columns of G. We therefore turn our attention to proving Theorem 3.1. The proof relies on the following equivalent definition of a ZK code.

Lemma 3.3 (ZK Codes, Equivalent Formulation)**.** *Suppose that $C \subseteq \mathbb{F}^n$ is a linear code of dimension k, let $G \in \mathbb{F}^{n \times k}$ be a generator matrix for C, and let $k' < k$ and $t < n$ be positive integers. Then the k'-randomized encoding map $\mathsf{Enc} : \mathbb{F}^{k'} \to C$ for G is t-ZK if and only if any linear combination of any t rows in G does not result in a non-zero $w \in \mathbb{F}^k$ such that $w|_{[k] \setminus [k']} = 0$.*

[1] Such a G exists since $C_Z^\perp \subseteq (C_X^\perp)^\perp = C_X$.

A similar characterization of ZK codes as in the above Lemma 3.3 was given in [BCL22, Lemma 5.1]. Here we provide an alternate self-contained proof. We also note that [ISVW13, Claim 6.1] show that the *stronger* condition that "any linear combination of t rows in G does not result in (*not* necessarily zero) $w \in \mathbb{F}^k$ such that $w|_{[k]\setminus[k']} = 0$" implies that Enc is t-ZK. Finally, we note that [BCL22, Lemma 5.2] showed that a similar condition to the latter is equivalent to the stronger property that Enc is *uniform* t-ZK. (Enc is *uniform t-ZK* if for any $\mathsf{m} \in \mathbb{F}^{k'}$ and for any $\mathcal{I} \subseteq [n]$ of size t, $\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}}$ is the uniform distribution over $\mathbb{F}^t$.)

Proof of Lemma 3.3: For $\mathcal{I} \subseteq [n]$, let $G|_{\mathcal{I}}$ denote the restriction of G to the rows in $\mathcal{I}$. It suffices to show that for any subset $\mathcal{I} \subseteq [n]$, $\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}} \equiv \mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}$ for any pair of messages $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$ if and only if any linear combination of the rows of $G|_{\mathcal{I}}$ does not result in a non-zero $w \in \mathbb{F}^k$ such that $w|_{[k]\setminus[k']} = 0$. We prove the lemma in two steps. First, we show (in Claim 3.4) that the former requirement "$\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}} \equiv \mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}$ for any $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$" is equivalent to requiring that "$0 \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ for any $\mathsf{m} \in \mathbb{F}^{k'}$". Then, we show (in Claim 3.5) that the requirement "$0 \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ for any $\mathsf{m} \in \mathbb{F}^{k'}$" is equivalent to the latter requirement "any linear combination of rows of $G|_{\mathcal{I}}$ does not result in $0 \neq w \in \mathbb{F}^k$ with $w|_{[k]\setminus[k']} = 0$". This will conclude the proof of the lemma.

Claim 3.4. *Let $\mathcal{I} \subseteq [n]$. Then $\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}} \equiv \mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}$ for any pair of messages $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$ if and only if $0 \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ for any $\mathsf{m} \in \mathbb{F}^{k'}$.*

Proof: For the 'only if' part, note that if $0 \notin \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ for some $0 \neq \mathsf{m} \in \mathbb{F}^{k'}$, then since $0 \in \mathsf{Supp}(\mathsf{Enc}(0)|_{\mathcal{I}})$, then we clearly have that $\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}} \not\equiv \mathsf{Enc}(0)|_{\mathcal{I}}$.

For the 'if' part, assume that $0 \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ for any $\mathsf{m} \in \mathbb{F}^{k'}$. Then in this case, for any $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$, we have that $0 \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m}' - \mathsf{m})|_{\mathcal{I}})$, and so by linearity,

$$\mathsf{Supp}(\mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}) \supseteq \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}}) + \mathsf{Supp}(\mathsf{Enc}(\mathsf{m}' - \mathsf{m})|_{\mathcal{I}}) \supseteq \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}}).$$

Indeed, the right containment uses the fact that $0 \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m}' - \mathsf{m})|_{\mathcal{I}})$. The left containment follows from linearity, because if $u := G|_{\mathcal{I}} \cdot (\mathsf{m}, r) \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ and $u' := G|_{\mathcal{I}} \cdot (\mathsf{m}' - \mathsf{m}, r') \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m}' - \mathsf{m})|_{\mathcal{I}})$, then $u + u' = G|_{\mathcal{I}} \cdot (\mathsf{m}', r + r') \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}})$. In summary, $\mathsf{Supp}(\mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}) \supseteq \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ for any pair of messages $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$, so we conclude that $\mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}}) = \mathsf{Supp}(\mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}})$ for any pair of messages $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$. Finally, observe that by properties of linear algebra, for any $\mathsf{m} \in \mathbb{F}^{k'}$, the number of $r \in \mathbb{F}^{k-k'}$ which satisfy the system of linear equations $G|_{\mathcal{I}} \cdot (\mathsf{m}, r) = v$ is the same for any $v \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$. Consequently, the fact that $\mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}}) = \mathsf{Supp}(\mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}})$ implies that $\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}} \equiv \mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}$, and we conclude that $\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}} \equiv \mathsf{Enc}(\mathsf{m}')|_{\mathcal{I}}$ for any pair of messages $\mathsf{m}, \mathsf{m}' \in \mathbb{F}^{k'}$. ■

Claim 3.5. *Let $\mathcal{I} \subseteq [n]$. Then $0 \in \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$ for any $\mathsf{m} \in \mathbb{F}^{k'}$ if and only if any linear combination of the rows of $G|_{\mathcal{I}}$ does not result in a non-zero $w \in \mathbb{F}^k$ such that $w|_{[k]\setminus[k']} = 0$.*

Proof: For the 'only if' part, suppose that there exists a linear combination $u \in \mathbb{F}^{|\mathcal{I}|}$ of the rows of $G|_{\mathcal{I}}$ which results in a non-zero $w \in \mathbb{F}^k$ such that $w|_{[k]\setminus[k']} = 0$, and let $j \in [k']$ be an entry so that $w_j \neq 0$. Let $\mathsf{m} \in \mathbb{F}^{k'}$ be the j-th unit vector. We shall show that there does not exist an $r \in \mathbb{F}^{k-k'}$ so that $G|_{\mathcal{I}} \cdot (\mathsf{m}, r) = 0$, and consequently $0 \notin \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$. To see the latter, suppose on the contrary that there exists an $r \in \mathbb{F}^{k-k'}$ so that $G|_{\mathcal{I}} \cdot (\mathsf{m}, r) = 0$. Then we have that

$$0 = \langle u, G|_{\mathcal{I}} \cdot (\mathsf{m}, r) \rangle = \langle (u^T \cdot G|_{\mathcal{I}})^T, (\mathsf{m}, r) \rangle = \langle w, (\mathsf{m}, r) \rangle = \langle w|_{[k']}, \mathsf{m} \rangle + \langle w|_{[k]\setminus[k']}, r \rangle = w_j + 0 = w_j \neq 0,$$

which is a contradiction.

For the 'if' part, suppose that there exists an $\mathsf{m} \in \mathbb{F}^{k'}$ so that $0 \notin \mathsf{Supp}(\mathsf{Enc}(\mathsf{m})|_{\mathcal{I}})$. Then the linear system $G|_{\mathcal{I}} \cdot (\mathsf{m}, r) = 0$ does not have a solution $r \in \mathbb{F}^{k-k'}$. Let A be the matrix which consists of the first k' columns of $G|_{\mathcal{I}}$, and let B be the matrix which consists of the last $k - k'$ columns of $G|_{\mathcal{I}}$. Then by properties of linear algebra, we have that there exists a linear combination $u \in \mathbb{F}^{|\mathcal{I}|}$ so that $\langle u, A \cdot \mathsf{m} \rangle = \langle (u^T \cdot A)^T, \mathsf{m} \rangle \neq 0$ but $u^T \cdot B = 0$. (Indeed, the system $G|_{\mathcal{I}} \cdot (\mathsf{m}, r) = 0$ is equivalent to the system $B \cdot r = -A \cdot \mathsf{m}$, where A, B, m are fixed.) But this implies in turn that $w := u^T \cdot G|_{\mathcal{I}} = (u^T \cdot A, u^T \cdot B)$ is a linear combination of the rows of $G|_{\mathcal{I}}$ which satisfies that $w|_{[k']} = u^T \cdot A \neq 0$, but $w|_{[k] \setminus [k']} = u^T \cdot B = 0$. ■

This concludes the proof of Lemma 3.3. ■

We now turn to the proof of Theorem 3.1, based on the above Lemma 3.3.

Proof of Thm 3.1: We prove each of the items separately.

Item (1): Follows since $C_X^\perp = C^\perp$, and $C_Z^\perp$ is the span of the last $k - k'$ columns of G, and so $C_Z^\perp \subseteq C$.

Item (2): Recall that Enc is decodable from e errors if and only if for any pair of distinct messages $\mathsf{m} \neq \mathsf{m}' \in \mathbb{F}^{k'}$ and (not necessarily distinct) $r, r' \in \mathbb{F}^{k-k'}$, it holds that $\Delta(G \cdot (\mathsf{m}, r), G \cdot (\mathsf{m}', r')) > 2e$. Further, by linearity, this latter property is equivalent to the property that for any non-zero $\mathsf{m} \in \mathbb{F}^{k'}$ and (possibly zero) $r \in \mathbb{F}^{k-k'}$ it holds that $\mathrm{wt}(G \cdot (\mathsf{m}, r)) > 2e$. Thus, it suffices to show that $d_X = \min_{0 \neq \mathsf{m} \in \mathbb{F}^{k'}, r \in \mathbb{F}^{k-k'}} \mathrm{wt}(G \cdot (\mathsf{m}, r))$.
But the above follows since

$$\begin{aligned} C_X \setminus C_Z^\perp &= \{c \in C_X \mid c \notin C_Z^\perp\} \\ &= \{c \in C \mid c \text{ is not in the span of the last } k - k' \text{ columns of } G\ \} \\ &= \{G \cdot (\mathsf{m}, r) \mid 0 \neq \mathsf{m} \in \mathbb{F}^{k'}, r \in \mathbb{F}^{k-k'}\}, \end{aligned}$$

and so $d_X = \min_{c \in C_X \setminus C_Z^\perp} \mathrm{wt}(c) = \min_{0 \neq \mathsf{m} \in \mathbb{F}^{k'}, r \in \mathbb{F}^{k-k'}} \mathrm{wt}(G \cdot (\mathsf{m}, r))$.

Item (3): By Lemma 3.3, Enc is t-ZK if and only if any linear combination of any t rows in G does not result in a non-zero $w \in \mathbb{F}^k$ such that $w|_{[k] \setminus [k']} = 0$. We shall show that the latter condition is equivalent to the condition that $d_Z > t$. To see this, note that a linear combination of t rows in G resulting in $w \in \mathbb{F}^k$, corresponds to a vector $u \in \mathbb{F}^n$ of weight at most t so that $u^T \cdot G = w$. Furthermore, the condition that $w \neq 0$ is equivalent to the condition that $u \notin C_X^\perp = C^\perp$, while the condition that $w|_{[k] \setminus [k']} = 0$ is equivalent to the condition that $u \in C_Z$. Thus, the condition that any linear combination of any t rows in G does not result in a non-zero $w \in \mathbb{F}^k$ such that $w|_{[k] \setminus [k']} = 0$ is equivalent to the condition that there do not exist $u \in C_Z \setminus C_X^\perp$ of weight at most t, which is equivalent to the condition that $d_Z > t$. ■

4 Application: Explicit Asymptotically-Good Zero-knowledge Locally-Testable Codes

We now describe an immediate application of the equivalence between ZK codes and quantum CSS codes of Section 3. Specifically, we use recent constructions of asymptotically-good locally testable quantum codes to obtain explicit asymptotically-good ZK codes that are also *locally testable* with a few queries. We first formally define locally-testable codes (LTCs).

Definition 4.1 (Locally-Testable Code (LTC))**.** *A code $C \subseteq \mathbb{F}^n$ is a q-*query Locally Testable Code *(q-*LTC*) if there exists a randomized oracle algorithm* TEST *which receives oracle access to a string $w \in \mathbb{F}^n$, makes q queries to w, and outputs either 'accept' or 'reject', so that the following conditions holds:*

- ***Completeness:*** *If $w \in C$ then* TEST *accepts with probability* 1*.*
- ***Soundness:*** *If $w \notin C$ then* TEST *rejects with probability at least $\frac{1}{4} \cdot \frac{\Delta(w,C)}{n}$.*

A ZK code that is also an LTC, with a ZK threshold that is significantly larger than the query complexity of the local tester, is called a *ZK-LTC*. Such codes lie at the heart of ZK-PCP and ZK-IOP constructions (and are also used in other cryptographic contexts such as verifiable secret sharing). Ishai et al. [ISVW13] gave a generic method of (probabilistically) transforming any linear code into a ZK code (Their probabilistic transformation outputs a generator matrix for the ZK code, with negligible probability of error.) They then use this transformation to obtain a *probabilistic* construction of asymptotically good ZK-LTCs. Combining new quantum LTC constructions [DLV24, KP25, WLH25], and the equivalence between quantum CSS codes and ZK codes, yields an *explicit* construction of asymptotically-good ZK-LTCs. This is formalized in Corollary 4.3 below. We first cite the relevant quantum LTCs (see [WLH25, Thm. 1.3 and Table 4], who build on the codes of [DLV24, KP25]):

Theorem 4.2 (Asymptotically-good quantum LTCs [DLV24, WLH25])**.** *There exists an explicit infinite family of CSS codes $C_X, C_Z \subseteq \mathbb{F}^n$, where (C_X, C_Z) has constant rate and distance $\Omega(n)$, and both C_X and C_Z are locally testable with $\mathsf{poly}\log(n)$ queries.*

Combining the above Theorem 4.2 with Corollary 3.2 gives explicit asymptotically-good ZK-LTCs with linear ZK threshold that are locally testable with a poly-logarithmic number of queries. To the best of our knowledge, this is the first instance of an explicit family of asymptotically-good ZK-LTCs in which the ZK threshold is larger than the tester's query complexity.

Corollary 4.3. *There exists an explicit infinite family of codes $\mathcal{C} = (C_n)_n$, where $C_n \subseteq \mathbb{F}^n$ is a linear code that is locally testable with $\mathsf{poly}\log(n)$ queries. Furthermore, there exist an explicit generator matrix G for C_n and $k' = \Theta(n)$, so that the k'-randomized encoding map $\mathsf{Enc} : \mathbb{F}^{k'} \to C_n$ for G is $\Omega(n)$-ZK, and is decodable from $\Omega(n)$ errors.*

Remark 4.4. *We note that quantum LTCs satisfy the stronger requirement that* both *C_X and C_Z are locally testable, while the application for ZK-LTCs only requires that $C = C_X$ is locally testable. In particular, while we do not know of asymptotically-good constant-query quantum LTCs, combining the transformation of [ISVW13] with the asymptotically-good constant-query classical LTCs of [DEL+22, PK22] gives a* probabilistic *construction of asymptotically-good ZK-LTCs, with linear ZK threshold and* constant *query complexity.*

Acknowledgement. We thank Louis Golowich, Thomas Vidick, and Gilles Zémor for discussions on the topic. The discussion leading to this note was initiated at the "Error-Correcting Codes: Theory and Practice Reunion" held at the Simons Institute for the Theory of Computing on April 2025. Research supported in part by a grant from the UC Noyce Initiative to the Simons Institute for the Theory of Computing.

Noga Ron-Zewi was partially supported by the European Union (ERC, ECCC, 101076663). Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Council. Neither the European Union nor the granting authority can be held responsible for them. The second author is supported by ISF grant No. 434/24.

References

[AALV09] Dorit Aharonov, Itai Arad, Zeph Landau, and Umesh Vazirani. The detectability lemma and quantum gap amplification. In *STOC*, page 417–426. Association for Computing Machinery, 2009.

[ABN23] Anurag Anshu, Nikolas P. Breuckmann, and Chinmay Nirkhe. NLTS hamiltonians from good quantum codes. In *STOC*, pages 1090–1096, 2023.

[AHIV17] Scott Ames, Carmit Hazay, Yuval Ishai, and Muthuramakrishnan Venkitasubramaniam. Ligero: Lightweight sublinear arguments without a trusted setup. In *CCS*, pages 2087–2104, 2017.

[ALM$^+$92] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and hardness of approximation problems. In *FOCS*, pages 14–23, 1992.

[AN02] Dorit Aharonov and Tomer Naveh. Quantum NP - a survey, 2002.

[AS92] Sanjeev Arora and Shmuel Safra. Probabilistic checking of proofs; A new characterization of NP. In *FOCS*, pages 2–13, 1992.

[BBHR19] Eli Ben-Sasson, Iddo Bentov, Yinon Horesh, and Michael Riabzev. Scalable zero knowledge with no trusted setup. In *CRYPTO*, pages 701–732, 2019.

[BCF$^+$17] Eli Ben-Sasson, Alessandro Chiesa, Michael A. Forbes, Ariel Gabizon, Michael Riabzev, and Nicholas Spooner. Zero knowledge protocols from succinct constraint detection. In *TCC, Proceedings, Part II*, pages 172–206, 2017.

[BCGV16] Eli Ben-Sasson, Alessandro Chiesa, Ariel Gabizon, and Madars Virza. Quasi-linear size zero knowledge from linear-algebraic PCPs. In *TCC 2016-A, Proceedings, Part II*, pages 33–64, 2016.

[BCL22] Jonathan Bootle, Alessandro Chiesa, and Siqi Liu. Zero-knowledge IOPs with linear-time prover and polylogarithmic-time verifier. In *EUROCRYPT*, pages 275–304, 2022.

[BCS16] Eli Ben-Sasson, Alessandro Chiesa, and Nicholas Spooner. Interactive oracle proofs. In *TCC 2016-B, Proceedings, Part II*, volume 9986 of *Lecture Notes in Computer Science*, pages 31–60, 2016.

[BGW88] Michael Ben-Or, Shafi Goldwasser, and Avi Wigderson. Completeness theorems for non-cryptographic fault-tolerant distributed computation (extended abstract). In *STOC*, pages 1–10, 1988.

[CCD88] David Chaum, Claude Crépeau, and Ivan Damgård. Multiparty unconditionally secure protocols (extended abstract). In *STOC*, pages 11–19. ACM, 1988.

[CCG$^+$07] Hao Chen, Ronald Cramer, Shafi Goldwasser, Robbert de Haan, and Vinod Vaikuntanathan. Secure computation from random error correcting codes. In *EUROCRYPT*, pages 291–310, 2007.

[CDN15] Ronald Cramer, Ivan Damgård, and Jesper Buus Nielsen. *Secure Multiparty Computation and Secret Sharing*. Cambridge University Press, 2015.

[CFGS18] Alessandro Chiesa, Michael A. Forbes, Tom Gur, and Nicholas Spooner. Spatial isolation implies zero knowledge even in a quantum world. In *FOCS*, pages 755–765. IEEE Computer Society, 2018.

[CFW26] Alessandro Chiesa, Giacomo Fenzi, and Guy Weissenbergu. Zero-knowledge IOPPs for constrained interleaved codes. Cryptology ePrint Archive, Report 2026/391, 2026. https://eprint.iacr.org/2026/391.

[CGKS95] Benny Chor, Oded Goldreich, Eyal Kushilevitz, and Madhu Sudan. Private information retrieval. In *FOCS*, pages 41–50. IEEE Computer Society, 1995.

[CS96] A. R. Calderbank and Peter W. Shor. Good quantum error-correcting codes exist. *Phys. Rev. A*, 54:1098–1105, 1996. https://link.aps.org/doi/10.1103/PhysRevA.54.1098.

[DEL$^+$22] Irit Dinur, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. Locally testable codes with constant rate, distance, and locality. In *STOC*, pages 357–374, 2022.

[DGR99] Scott E. Decatur, Oded Goldreich, and Dana Ron. Computational sample complexity. *SIAM J. Comput.*, 29(3):854–879, 1999.

[DGR20] Scott E. Decatur, Oded Goldreich, and Dana Ron. A probabilistic error-correcting scheme that provides partial secrecy. In *Computational Complexity and Property Testing - On the Interplay Between Randomness and Computation*, pages 1–8. Springer, 2020. *(Original version appeared already in 1997 on Cryptology ePrint Archive, Report 1997/005).*

[DLV24] Irit Dinur, Ting-Chun Lin, and Thomas Vidick. Expansion of higher-dimensional cubical complexes with application to quantum locally testable codes. In *FOCS*, pages 379–385. IEEE, 2024.

[FMSS04] Jon Feldman, Tal Malkin, Rocco A. Servedio, and Cliff Stein. Secure network coding via filtered secret sharing. In *Proceedings of the 42nd Annual Allerton Conference on Communication, Control, and Computing*, 2004.

[GOS25] Tom Gur, Jack O'Connor, and Nicholas Spooner. A zero-knowledge PCP theorem. In *STOC*, pages 986–994. ACM, 2025.

[ISVW13] Yuval Ishai, Amit Sahai, Michael Viderman, and Mor Weiss. Zero knowledge LTCs and their applications. In *RANDOM*, pages 607–622, 2013.

[KP25] Gleb Kalachev and Pavel Panteleev. Maximally extendable product codes are good coboundary expanders. In *FOCS*, pages 1512–1524. IEEE, 2025.

[LRR19] Felipe Gomes Lacerda, Joseph M. Renes, and Renato Renner. Classical leakage resilience from fault-tolerant quantum computation. *J. Cryptol.*, 32(4):1071–1094, 2019.

[PK22] Pavel Panteleev and Gleb Kalachev. Asymptotically good quantum and locally testable classical LDPC codes. In *STOC*, pages 375–388, 2022.

[RRR16] Omer Reingold, Guy N. Rothblum, and Ron D. Rothblum. Constant-round interactive proofs for delegating computation. In *STOC*, pages 49–62. ACM, 2016.

[RW24] Noga Ron-Zewi and Mor Weiss. Zero-knowledge IOPs approaching witness length. In *CRYPTO, Proceedings, Part X*, volume 14929 of *Lecture Notes in Computer Science*, pages 105–137. Springer, 2024.

[Sha79] Adi Shamir. How to share a secret. *Commun. ACM*, 22(11):612–613, 1979.

[Ste96] Andrew Steane. Multiple-particle interference and quantum error correction. *Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences*, 452(1954):2551–2577, 11 1996. https://doi.org/10.1098/rspa.1996.0136.

[WLH25] Adam Wills, Ting-Chun Lin, and Min-Hsiu Hsieh. Tradeoff constructions for quantum locally testable codes. *IEEE Transactions on Information Theory*, 71(1):426–458, 2025.

ECCC ISSN 1433-8092

https://eccc.weizmann.ac.il