On the existence of good locally testable error-correcting codes

Bogdan Grechuk • 10 Mar 2026

The March 2026 issue of the Annals of Mathematics contains a paper by Dinur, Evra, Livne, Lubotzky, and Mozes (Dinur et al. 2026) presenting an explicit construction of error-correcting codes with constant rate, constant relative distance, and local testability with constant locality and testability parameters. This result resolves a long-standing central open problem in the theory of error-correcting codes.

An error-correcting code is a method for protecting information transmitted through a noisy communication channel. As a simple example, suppose we want to transmit a message of length k consisting of symbols 0 and 1. One strategy is to replace each symbol $x \in \{0,1\}$ with a block of $2m+1$ identical symbols x. If at most m symbols in each block are corrupted during transmission, the receiver can recover the original symbol by taking the majority value within the block. In this example, the length of the encoded message becomes $n = (2m+1)k$.

In general, an error-correcting code is an injective function $L : \{0,1\}^k \to \{0,1\}^n$ for some $k \le n$, where $\{0,1\}^n$ denotes the set of binary strings $x = (x_1, \dots, x_n)$ of length n. Let $C \subset \{0,1\}^n$ denote the image of L. The integer $n = n(L)$ is called the *length* of the code, while the ratio

$$r(L) = \frac{\log_2 |C|}{n} = \frac{k}{n}$$

is called the *rate* of the code.

For two strings $x, y \in \{0,1\}^n$, define their relative distance by

$$\Delta(x,y) = \frac{|\{1 \le i \le n : x_i \ne y_i\}|}{n}.$$

The *relative distance* of the code L is

$$d(L) = \min_{x \ne y \in C} \Delta(x,y),$$

that is, the minimal relative distance between two distinct codewords.

The receiver knows in advance that only strings from C may be transmitted. If the distance between any two codewords is at least $2m+1$, and at most m symbols are corrupted during transmission, then the receiver can uniquely determine which codeword $x \in C$ was sent by choosing the closest codeword to the received string. This discussion shows that desirable codes should simultaneously have high rate $r(L)$ (allowing many messages to be encoded) and large relative distance $d(L)$ (allowing many errors to be corrected).

A family of error-correcting codes L_i with lengths $n(L_i) \to \infty$ is called *good* if there exist universal constants $\rho, \delta > 0$ such that

$$r(L_i) \geq \rho \quad \text{and} \quad d(L_i) \geq \delta$$

for all i. It is known (Blokh and Zyablov 1973) that such codes exist whenever ρ and δ satisfy the Gilbert–Varshamov bound

$$\rho + h(\delta) < 1,$$

where $h(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function.

Another highly desirable property of an error-correcting code is *local testability*. Given an integer $q > 0$ and a real number $\kappa > 0$, we say that a code L with image $C \subset \{0,1\}^n$ is (q,κ)-locally testable if there exists a probabilistic algorithm that reads at most q bits of a string $x \in \{0,1\}^n$ and outputs 1 or 0 such that

- If $x \in C$, the algorithm outputs 1 with probability 1.
- If $x \in \{0,1\}^n \setminus C$, then the algorithm outputs 0 with probability at least $\kappa \cdot \Delta_C(x)$, where

  $$\Delta_C(x) = \min_{y \in C} \Delta(x,y)$$

  is the relative distance from x to the nearest codeword.

The rejection probability $\kappa \cdot \Delta_C(x)$ can be amplified arbitrarily by repeating the test multiple times. Therefore, if L is (q,κ)-locally testable with parameters q and κ independent of n, we can determine whether $x \in C$ extremely quickly and with high confidence. The parameter $q = q(L)$ is called the *locality* of the code, while $\kappa = \kappa(L)$ is called the *testability parameter*.

A central open problem in the area has been whether there exist error-correcting codes that simultaneously have constant rate, constant relative distance, and local testability with constant locality and testability parameters. The recent paper (Dinur et al. 2026) (and independently (Panteleev and Kalachev 2022)) answers this question affirmatively.

Theorem 1 *For any $0 < \rho < 1$, there exist constants $\delta_\rho > 0$, $\kappa_\rho > 0$, and $q_\rho \in \mathbb{N}$, and an infinite family of explicitly constructed locally testable codes $\{L_i\}$ with lengths $n(L_i) \to \infty$ such that for every i,*

$$r(L_i) \geq \rho, \qquad d(L_i) \geq \delta_\rho, \qquad q(L_i) = q_\rho, \qquad \kappa(L_i) \geq \kappa_\rho.$$

Moreover, the images C_i of L_i are linear subspaces of $\{0,1\}^{n(L_i)}$, and bases for these subspaces can be found in time polynomial in $n(L_i)$.

Theorem 1 not only establishes the existence of codes with constant rate, relative distance, and locality, but also shows that the rate can be made arbitrarily close to 1, while the codes remain explicitly constructible in polynomial time. Furthermore, combining Theorem 1 with the main result of (Gopi et al. 2018) implies that the existence statement remains valid for any $\delta_\rho > 0$ satisfying the Gilbert–Varshamov condition $\rho + h(\delta_\rho) < 1$, although a deterministic polynomial-time construction is not known throughout this entire range. Finally, one can choose parameters satisfying

$$q_\rho \leq P_1(\epsilon^{-1}), \qquad \kappa_\rho \geq \frac{1}{|P_2(\epsilon^{-1})|},$$

for some polynomials P_1, P_2, where $\epsilon = 1 - \rho - h(\delta_\rho)$.

References

Blokh, È L, and Victor Vasilievich Zyablov. 1973. “Existence of Linear Concatenated Binary Codes with Optimal Correcting Properties.” *Problemy Peredachi Informatsii* 9 (4): 3–10.

Dinur, Irit, Shai Evra, Ron Livne, Alexander Lubotzky, and Shahar Mozes. 2026. “Good Locally Testable Codes.” *Ann. Of Math. (2)* 203 (2). https://doi.org/10.4007/annals.2026.203.2.3.

Gopi, Sivakanth, Swastik Kopparty, Rafael Oliveira, Noga Ron-Zewi, and Shubhangi Saraf. 2018. “Locally Testable and Locally Correctable Codes Approaching the Gilbert-Varshamov Bound.” *IEEE Trans. Inform. Theory* 64 (8): 5813–31. https://doi.org/10.1109/TIT.2018.2809788.

Panteleev, Pavel, and Gleb Kalachev. 2022. “Asymptotically Good Quantum and Locally Testable Classical LDPC Codes.” *STOC ’22—Proceedings of the 54th Annual ACM SIGACT Symposium on Theory of Computing*, 375–88.