Improved Decoding of Tanner Codes

Zhaienhe Zhou
University of Science and Technology of China

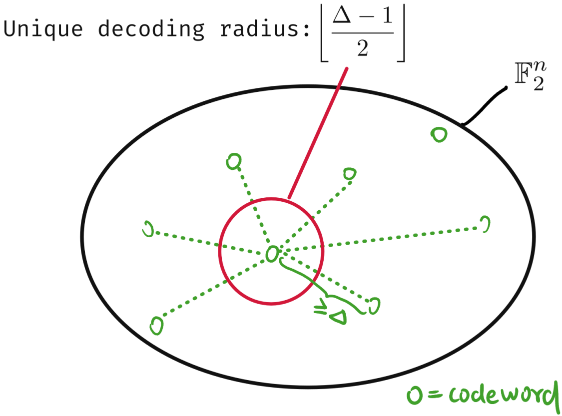
Zeyu Guo
The Ohio State University

ISIT 2025
June 26, 2025

Intro: Codes

Definition (Linear Code)

A linear code $C = \{C_1, C_2 \ldots\} \subseteq \mathbb{F}_2^n$ has a set of codewords that forms a **linear subspace**.
Its distance is defined as $\Delta := \min_{i \neq j} d_H(C_i, C_j)$.

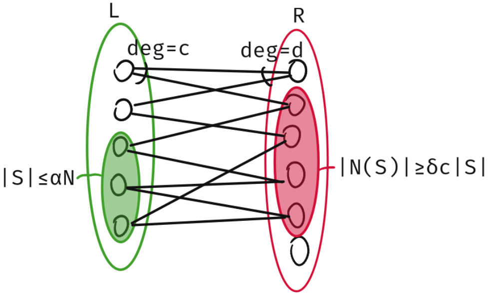


Intro: Expander

Definition (Bipartite Expander)

(c, d, α, δ)-bipartite expander:

- (c, d)-regular bipartite graph $G = (L \cup R, E)$
- $\forall$ vertex set $S \subseteq L$ with $|S| \leq \alpha n$, it holds that $|N(S)| \geq \delta c|S|$. Where $n := |L|$.

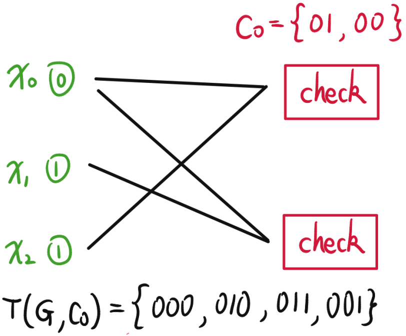


Note: treat c, d, α, δ as constant

Intro: Expander Codes

Definition (Expander Codes)

Let G be a (c, d, α, δ)-bipartite expander. C_0 is a fixed linear **inner code** of length d (**same as the degree**) and distance d_0.
A codeword of $T(G, C_0)$ is an assignment of bits to vertices in L such that for each $v \in R$, the **vector of bits on its neighbors** forms a codeword in C_0.



Motivation: Build longer codes base on C_0.
Challenge: A check node might be adjacent to many corrupted bits, running local (inner code) decoding may not correct it.

Intro: Problem

- **Goal:** Decode $\Omega(n)$ errors in linear time.
- **Central Question:** What conditions on the inner code distance (d_0) and graph expansion (δ) are sufficient?

Related Work: Linear-time Decoding

C_0	Work	Regime	Radius
Parity ($d_0 = 2$)	[SS96]	$\delta > \frac{3}{4}$	$(2\delta - 1)\alpha n$
	[Vid13]	$\delta > \frac{2}{3}$	$\frac{3\delta-2}{2\delta-1}\alpha n$
	[CCLO23]	$\delta > \frac{3}{4}$	$\delta\alpha n$ + size-expansion tradeoff
General	[DG18]	$d_0\delta^2 > \Omega(c)$	αn
	[COSS24]	$d_0\delta > 3$	αn (rand) $\frac{2\alpha}{d_0(1+0.5c\delta)} n$
	Ours	$d_0\delta > 2$	αn

Fundamental Limit [Vid13, COSS24]: Decoding is impossible if $d_0\delta \leq 1$.

Result 1: Randomized Decoding

Theorem (Randomized Decoding)

Randomized *algorithm that can correct* αn *errors in* $O(n)$ *time for any Expander code* $T(G, C_0)$ *satisfying* $\delta d_0 > 2$.

- α: Set size in the definition of expansion
- δ: Expansion rate
- d_0: Distance of C_0

Result 1: RandFlip Algorithm

- Each unsatisfied check $\in R$ sends a weight to one of its adjacent "wrong" bits (**bits flipped in local decode**)
- The more "wrong" bits, the **less** weight it sends
- Flip each bit with a probability **proportional to the sum of the weights** it receives

Theorem (3.2, Correct Constant Fraction Errors)

Let y = **the closest codeword** *in $T(G, C_0)$, then after RandFlip:*

$$\mathbb{E}\left[d_H(x', y)\right] \leq \left(1 - \frac{\varepsilon_0 \delta}{t}\right) d_H(x, y)$$

where $t = \frac{d_0}{2}$ (unique decoding radius of C_0) and $\varepsilon_0 = \frac{d_0}{2} - \frac{1}{\delta} > 0$ (guaranteed by $d_0\delta > 2$).

Result 1: Algorithm

Algorithm 1 RandFlip(x)

$t \leftarrow \frac{d_0}{2}$, $(p_1, \dots, p_n) \leftarrow (0, \cdots, 0) \in \mathbb{R}^n$
for each $v \in R$ **do**
    $w_v \leftarrow \mathrm{Decode}(x_{n(v)})$
    if $1 \le d_H(w_v, x_{N(v)}) < t$ **then**
        Choose any $i \in N(v)$ where w_v and $x_{N(v)}$ differ
        $p_i \leftarrow p_i + \frac{t - d_H(w_v, x_{N(v)})}{ct}$ ▷ Weighted voting allows $\delta d_0 > 2$
    end if
end for
for each $i \in [n]$ **do**
    Flip x_i with probability p_i
end for
return x

Final algorithm: RandFlip $O(\log n)$ times

Result 1: Proof Sketch

F: Set of corrupted bits ($|F| \leq \alpha n$)

$N_k(F)$: Check nodes with *exactly* k neighbors in F

$$\sum_{k=1}^{d} k|N_k(F)| = c|F|, \quad \sum_{k=1}^{d} |N_k(F)| \geq \delta c|F|.$$

(Expansion Property)

Multiplying the second by $t = \frac{1}{\delta} + \varepsilon_0$ and subtracting the first:

$$\sum_{k=1}^{d} (t-k)|N_k(F)| \geq \varepsilon_0 \delta c|F|.$$

Key Observation:

Contribution of a vertex in $N_k(F)$ to the expectation is at least $\frac{t-k}{ct}$.

Result 1: Proof Sketch

Lemma (3.3, Guarantees on false local decode)

For $v \in N_k(F)$ with $w := Decode(x_{N(v)})$:

- *If $w = y_{N(v)}$ (Correct C_0 codeword): $d_H(w, x_{N(v)}) = k$*
- *If $w \neq y_{N(v)}$ (Alternate C_0 codeword): $d_H(w, x_{N(v)}) \geq d_0 - k$*

Recall: sent weight$=\frac{t-d_H(w_v,x_{N(v)})}{ct}$.

- Wrong votes are sent **only when** $w \neq y_{N(v)}$
- Lemma 3.3 **bounds the negative contribution** of a wrong vote.

Limitations of the "Local Unique Decoding" Approach

Informal Remark (Necessary Condition)

$\delta d_0 > 2$ is necessary for the "Local Unique Decoding" approach

- Possible that $|F| = \alpha n$, $|N(F)| = \frac{2}{d_0} c|F|$
- Each $v \in N(F)$ is a neighbor of exactly $\frac{d_0}{2}$ bits in F, unable to unique decode.

Open Question

"Can't unique decode" its self still provides useful information, e.g. when C_0=parity check code. Can we extend the techniques?

Result 2: Deterministic Decoding

Theorem (Deterministic Decoding)

Deterministic *algorithm that can correct* αn *errors in* $O(n)$ *time for any Expander code* $T(G, C_0)$ *with* $\delta d_0 > 2$.

Derandomization Idea in [COSS24]:

DeterFlip: Flip all bits that receive a specific amount of weight

- Correct votes have $\Omega(|F|)$ **advantage** over incorrect votes
- Constant number $(O(cd_0) = O(1))$ of choices
- $\exists$ Choice that reduces $\Omega(F)$ errors (don't know which)

DeepFlip (repeat): Search $O(1)$-length sequence of choices

- $U :=$ **set of unsatisfied check**, $c_1|U| \le |F| \le c_2|U|$ by expansion (**loosely proportional**)
- prune if $|U| > c_3 n$, guarantee $|F| < \alpha n$
- preserve the branch that $|U|$ decreased the most (guarantees a constant fraction reduction in $|F|$)

Result 2: A loss in decoding radius

Why [COSS24] need $|F_{\textbf{initial}}| < \frac{2\alpha}{d_0(1+0.5c\delta)} n < \alpha n$**?**

$$\text{Prune condition: } |U| > c_3 n$$
$$\text{Guarantee: } |F| \leq \alpha n \text{ and thus } \delta\text{-expansion.}$$

Leave a "safety margin": Otherwise, one can't distinguish between $F_{initial}$ and $|F| > \alpha n$ ($|U|$ and $|F|$ is **loosely proportional**).

Result 2: Preliminary Search

Preliminary Search before the entire algorithm:

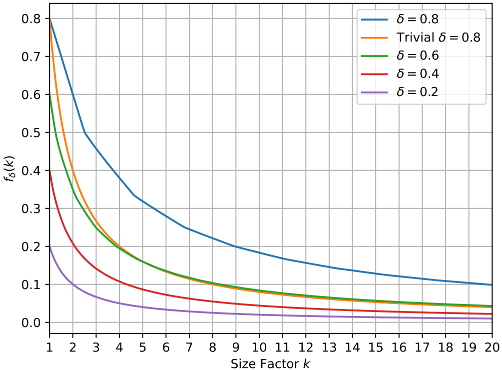
1. Search $r = O(1)$ steps of DeterFlip choices (without pruning)
2. **Guarantee:**
   - At least one branch reduces $|F|$ from αn to $\leq \frac{2\alpha}{d_0(1+0.5c\delta)} n$ (don't know which)
   - $O(1)^r = O(1)$ branches
3. Repeatedly DeepFlip on all branches simultaneously,
   - prune a branch when its time exceeds $O(n)$
   - verify the final decoding result (distance to initial vector x)

Result 3: Tool – Size-Expansion tradeoff

Lemma (Size-Expansion Tradeoff [CCLO23])

Any (c, d, α, δ)-bipartite expander is also a $(c, d, k\alpha, f_\delta(k))$-bipartite expander, where $k > 1$ is a constant, $f_\delta(k)$ is defined by a LP (omitted).

Larger set $\implies$ weaker expansion, better than trivial bound $\frac{\delta}{k}$



Result 3: Distance Bound & Decoding Radius

Theorem (Tight Distance Bound in General C_0)

The distance of the Expander code $T(G, C_0)$ is:

- *lower bounded by $f_\delta^{-1}(\frac{1}{d_0})\alpha n$*
- *"upper bounded by $(1 + o(1))f_\delta^{-1}(\frac{1}{d_0})\alpha n$" for sufficiently small α (construction on **regular graph**)*

Generalizes the bound for $C_0 =$ parity check code from [CCLO23]

Theorem (Improved Decoding Radius)

Suppose $\delta d_0 > 2$. Our algorithm can decode up to $f_\delta^{-1}\left(\frac{2}{d_0}\right)\alpha n$ errors in $O(n)$ time.

Stronger expansion $(\delta) \implies$ larger decoding radius.

Thank you!