

List-Recovery of Random Linear Codes over Small Fields

Dean Doron^{*} Jonathan Mosheiff[†] Nicolas Resch[‡] João Ribeiro[§]

Abstract

We study list-recoverability of random linear codes over small fields, both from errors and from erasures. We consider codes of rate ε -close to capacity, and aim to bound the dependence of the output list size L on ε , the input list size ℓ , and the alphabet size q . Prior to our work, the best upper bound was $L = q^{O(\ell/\varepsilon)}$ (Zyablov and Pinsker, Prob. Per. Inf. 1981).

Previous work has identified cases in which *linear* codes provably perform worse than non-linear codes with respect to list-recovery. While there exist non-linear codes that achieve $L = O(\ell/\varepsilon)$, we know that $L \geq \ell^{\Omega(1/\varepsilon)}$ is necessary for list recovery from erasures over fields of small characteristic, and for list recovery from errors over large alphabets.

We show that in other relevant regimes there is no significant price to pay for linearity, in the sense that we get the correct dependence on the gap-to-capacity ε and go beyond the Zyablov–Pinsker bound for the first time. Specifically, when q is constant and ε approaches zero,

- For list-recovery from erasures over *prime fields*, we show that $L \leq C_1/\varepsilon$. By prior work, such a result cannot be obtained for low-characteristic fields.
- For list-recovery from errors over *arbitrary fields*, we prove that $L \leq C_2/\varepsilon$.

Above, C_1 and C_2 depend on the decoding radius, input list size, and field size. We provide concrete bounds on the constants above, and the upper bounds on L improve upon the Zyablov–Pinsker bound whenever $q \leq 2^{(1/\varepsilon)^c}$ for some small universal constant $c > 0$.

^{*}Ben-Gurion University of the Negev. deand@bgu.ac.il.

[†]Ben-Gurion University of the Negev. mosheiff@bgu.ac.il.

[‡]Informatics Institute, University of Amsterdam. n.a.resch@uva.nl.

[§]Instituto de Telecomunicações and Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa. jribeiro@tecnico.ulisboa.pt.

1 Introduction

Error-correcting codes enable reliable communication over noisy channels by encoding messages $m \in \Sigma^k$ as codewords $c \in \Sigma^n$. A code $\mathcal{C} \subseteq \Sigma^n$ of rate $R = k/n$ and minimum (relative) Hamming distance δ allows for reliable communication over an adversarial noisy channel that corrupts up to a $\delta/2$ -fraction of codeword symbols. To tolerate more corruptions, one can relax unique decoding to *list decoding*, where the decoder outputs all codewords within a given Hamming radius.

This notion is further generalized by *list recovery (from errors)*, which models scenarios where the receiver gets a small list of possible values for each symbol. Formally, a code \mathcal{C} is said to be (ρ, ℓ, L) -*list-recoverable* if for every sequence of sets $T_1, \dots, T_n \subseteq \Sigma$ with $|T_i| \leq \ell$, we have

$$|\mathcal{C} \cap B_\rho(T_1 \times \dots \times T_n)| \leq L,$$

where $B_\rho(T_1 \times \dots \times T_n)$ denotes the Hamming ball consisting of all words in Σ^n that agree with T_1, \dots, T_n in at least $(1-\rho)n$ coordinates. When $\ell = 1$, list-recovery from errors reduces to standard list-decoding (from errors).

A related variant is *list recovery from erasures*, where some coordinates are entirely unknown, modeled by setting $T_i = \Sigma$. A code is said to be (α, ℓ, L) -*list-recoverable from erasures* if

$$|\mathcal{C} \cap (T_1 \times \dots \times T_n)| \leq L$$

whenever $|T_i| \leq \ell$ for at least $(1-\alpha)n$ positions. Here too, the case $\ell = 1$ corresponds to list-decoding from erasures.

List recoverable codes are used as a building block for list-decodable and uniquely decodable codes [GI02, GI03, GI04, GI05, KMRS17, GKO⁺18, HRW20]. They have also gained a significant independent interest, in part due to their applications in pseudorandomness [TZ04, GUV09, DMOZ22, KT22], algorithms (in particular, for heavy hitters, compressed sensing, and combinatorial group testing [INR10, NPR11, LNNT16, GLPS17, DW22]), and cryptography [HIOS15, HLR21].

For both list-recovery from errors and from erasures, there exists a well-defined *capacity threshold* that characterizes the maximal achievable rate for which bounded list-size decoding is possible. Specifically, given parameters ρ , ℓ , and alphabet size q , there is a critical rate $R^* = R^*(\rho, \ell, q)$ such that:

- For every $\varepsilon > 0$ and any large enough block length, there exist codes of rate $R^* - \varepsilon$ that are (ρ, ℓ, L) -list-recoverable (from errors or erasures) with

$$L = O_{\ell, \varepsilon}(1). \tag{1}$$

- For every $\varepsilon > 0$ and any large enough block length n , no code of rate $R^* + \varepsilon$ is (ρ, ℓ, L) -list-recoverable for $L = q^{o(n)}$.

The exact threshold depends on the recovery model:

- For (ρ, ℓ, L) -list-recoverability from *errors*, the threshold rate is

$$R_{\text{errors}}^* = 1 - h_{q, \ell}(\rho),$$

where

$$h_{q, \ell}(\rho) = \rho \log_q \left(\frac{q - \ell}{\rho} \right) + (1 - \rho) \log_q \left(\frac{\ell}{1 - \rho} \right),$$

valid for $0 \leq \rho \leq 1 - \frac{\ell}{q}$ [Res20, Theorem 2.4.12].

- For (α, ℓ, L) -list-recoverability from *erasures*, the corresponding threshold is

$$R_{\text{erasures}}^* = (1 - \alpha) \cdot (1 - \log_q \ell).$$

The dependence of the list size L on the parameters ℓ and ε (see Equation (1)) is often critical, and has been the focus of extensive research (e.g., [RW14, RW18, LP20, GLS⁺21, GLM⁺22, GST22, Tam24, CZ24, LS25]).

Using the probabilistic method, it is easy to show that plain random codes achieve $L = O(\ell/\varepsilon)$, and this dependence is often viewed as the optimal benchmark. Codes achieving this tradeoff are said to match the *Elias bound for list-recovery*, in reference to the analogous threshold in list-decoding [Eli57] (see also [MRSY24]).

To set expectations for list-recovery of *linear* codes, we recall the classic argument of Zyablov and Pinsker [ZP81], adapted to the setting of list-recovery by Guruswami [Gur03]. Since any set of $L + 1$ vectors has a linearly independent subset of size $\log_q(L + 1)$, and since the events that linearly independent vectors lie in a linear code are stochastically independent, the argument for plain random codes gives $L = q^{O(\ell/\varepsilon)}$. This naturally raises the question: what is the actual *price of linearity* in list-recovery? While various forms of degradation are possible, we seek to understand how the requirement of linearity affects the list-size achievable near capacity.

Prior work Most previous results concerning the output list size have focused on the *large alphabet regime*, where q is at least exponential in $1/\varepsilon$. In this setting, Li and Shagrithaya [LS25] recently proved that random linear codes are almost surely list-recoverable with list size $L \leq (\ell/\varepsilon)^{O(\ell/\varepsilon)}$. By a reduction between code ensembles [LMS24], the same upper bound also holds with high probability for Reed–Solomon codes over random evaluation sets. On the other hand, [LS25] proved that all (ρ, ℓ, L) -list-recoverable (from errors) linear codes over a large alphabet must satisfy $L \geq \ell^{\Omega(R/\varepsilon)}$, implying an exponential gap in the list-size between linear codes and plain random codes. A similar negative result was previously proven by Chen and Zhang [CZ24] for Reed–Solomon codes and folded Reed–Solomon codes. Recently, Komech and Mosheiff [KM25] constructed a new ensemble of non-linear codes that achieve $L \leq O(\ell/\varepsilon)$ in list-recovery from errors. These are the only codes other than plain random codes known to achieve the list-recovery Elias bound.

Older works of Rudra and Wootters [RW14, RW18], incomparable to [LS25], show (in our terms) that random linear codes achieve list-size $L \leq \ell^{\frac{1}{\varepsilon} \cdot \log^2(\ell/\varepsilon)}$ for list-recovery (from errors) in the large alphabet regime, but only under the guarantee that $\rho = 1 - \Omega(\varepsilon)$.

Other works concern the list-recoverability of folded Reed–Solomon codes, multiplicity codes, tensor codes, and variants of them (e.g., [KRSW18, HRW20, Tam24]). In particular, Tamo [Tam24] shows that folded Reed–Solomon codes and multiplicity codes achieve list size $L \leq (\ell/\varepsilon)^{O(\frac{1+\log \ell}{\varepsilon})}$ (in the errors case) in the large alphabet regime.

In contrast, very little is known about list-recovery in the *small alphabet regime*, where q is sub-exponential in $1/\varepsilon$. To the best of our knowledge, the only positive result in this setting is the aforementioned $L = q^{O(\ell/\varepsilon)}$ for random linear codes [ZP81]. On the other hand, we know that when q is a power of a small prime, random linear codes in this regime are very unlikely to be (α, ℓ, L) -list-recoverable from erasures with $\ell^{o(1/\varepsilon)}$ [GLM⁺22] (we state this as Theorem 1.1 below).

Provable separation between linear and nonlinear codes were also established in the setting of list decoding from erasures. For the special case of \mathbb{F}_2 , and aiming for an erasure decoding radius of $\alpha = 1 - \varepsilon$, Guruswami [Gur03] showed that the output list size must satisfy $L = \Omega(1/\varepsilon)$, as long as the rate is sufficiently non-vanishing. In contrast, plain random codes achieve $L = O(\log(1/\varepsilon))$, and we even have explicit constructions that nearly match plain random codes in some parameter regimes [BDT20].

1.1 Our Contribution

We establish new upper bounds on the output list size for list-recovery of random linear codes near capacity in the small alphabet regime. To the best of our knowledge, these are the only known bounds for general list-recovery in this setting beyond the classical Zyablov–Pinsker argument. Notably, our results achieve list sizes with only linear dependence on $1/\varepsilon$, in contrast to the exponential dependence in previous bounds.

List-recovery from erasures over prime fields. For our first result, we consider (α, ℓ, L) -list-recovery from erasures. Recall that the capacity in this case is

$$R_{\text{erasures}}^*(\alpha, \ell, q) = (1 - \alpha)(1 - \log_q \ell).$$

As mentioned before, [GLM⁺22] showed that there is a price to pay for linearity over fields of small characteristic. More precisely, they proved the following.

Theorem 1.1 (informal; see [GLM⁺22, Theorem III.1]). *If ℓ divides $\text{char}(\mathbb{F}_q)$, then with high probability over the choice of the linear code, the output list size L cannot be taken smaller than $\ell^{\Omega(1/\varepsilon)}$.*

We show that this limitation disappears when considering a *prime* field size q . In this case, we can make the output list size $O_{\alpha, \ell, q}(1/\varepsilon)$.

Theorem 1.2 (list recovery from erasures over prime fields; see Theorem 3.5). *Given $1 \leq \ell \leq q$ with q prime and $\alpha \in [0, 1)$, there exists $C(\alpha, \ell, q) > 0$ such that the following holds. Let $\mathcal{C} \leq \mathbb{F}_q^n$ be a random linear code of rate $R_{\text{erasures}}^*(\alpha, \ell, q) - \varepsilon$ for some $\varepsilon > 0$. Then, \mathcal{C} is with high probability $(\alpha, \ell, \frac{C(\alpha, \ell, q)}{\varepsilon})$ -list-recoverable from erasures.*

While our focus is on the setting where α and q are constants, we determine effective bounds on $C(\alpha, \ell, q)$ even when α is a function of n , and q is slightly super-constant.¹

List-recovery from errors. Next, we consider the case of list-recovery from errors, where we recall the capacity is

$$R_{\text{errors}}^*(\rho, \ell, q) = 1 - h_{q, \ell}(\rho).$$

Here, contrary to what happens in the regime of large q -s, we do not observe any price to pay for linearity, at least in terms of the dependence on the gap-to-capacity ε .

Theorem 1.3 (list recovery from errors; see Theorem 4.7). *Given $1 \leq \ell \leq q$ with q a prime power and $\rho \in (0, 1 - \ell/q)$, there exists $C(\rho, \ell, q) > 0$ such that the following holds. Let $\mathcal{C} \leq \mathbb{F}_q^n$ be a random linear code of rate $R_{\text{errors}}^*(\rho, \ell, q) - \varepsilon$ for some $\varepsilon > 0$. Then, \mathcal{C} is with high probability $(\rho, \ell, \frac{C(\rho, \ell, q)}{\varepsilon})$ -list-recoverable from errors.*

Again, we determine effective bounds on the numerator $C(\rho, \ell, q)$, which can be found in Theorem 4.7.² For context, we recall that in the “large q regime” (say, $q \gg \ell^{1/\varepsilon}$), such a result is provably impossible. Specifically, when q is large, the list-recovery capacity is (essentially) the Singleton bound, namely, $R_{\text{errors}}^* \approx 1 - \rho$. It is known that at rate $1 - \rho - \varepsilon$, *any* linear code

¹For a concrete example, when $\ell \leq (1 - \gamma)q$ for some constant γ , and α is bounded away from 1, we can take $C(\alpha, \ell, q) \leq q^{O(\ell \cdot \log q)}$ as long as $n \geq C(\alpha, \ell, q)$. We refer the reader to Theorem 3.5 for the precise bound.

²Specifically, when ρ is bounded away from both 0 and $1 - \ell/q$, we can take $C(\rho, \ell, q) \leq q^{\ell \cdot \text{polylog}(q)}$. See Theorem 4.7 for the precise bound.

list-recoverable from errors must have $L \geq \ell^{\Omega(R/\varepsilon)}$ [LS25]. That is, the dependence of L on the gap-to-capacity *must be exponential*. But in our case, at least if ρ, ℓ and q are held constant, the dependence of L on ε is just $O(1/\varepsilon)$.

We conclude this section with some remarks.

Remark 1.4 (on the field insensitivity). Both of our results show that there is no significant price to pay for linearity in list-recovery for certain parameter regimes. Our result in [Theorem 1.3](#) on list-recovery from errors is insensitive to the field size. On the other hand, as discussed above, our result in [Theorem 1.2](#) on list-recovery from erasures is (necessarily!) field sensitive. We provide some informal discussion on why this happens. First, note that we work with rates close to capacity, and the capacity in the erasures setting is larger for comparable α and ρ . Second, looking ahead (see [Section 1.2](#) for more details), list-recovery from erasures depends on the “additive structure” of $T_1 \times \cdots \times T_n$, for arbitrary size- ℓ subsets $T_1, \dots, T_n \subseteq \mathbb{F}_q$. If the T_i ’s are *subspaces* of \mathbb{F}_q , then it is quite likely these form a bad configuration for list-recovery from erasures. In contrast, list-recovery from errors depends on the additive structure of the “puffed-up” combinatorial rectangles

$$B_\rho(T_1 \times T_2 \times \cdots \times T_n) = \{x \in \mathbb{F}_q^n : x_i \notin T_i \text{ for at most } \rho n \text{ choices of } i \in [n]\}.$$

Even if the T_i ’s are subspaces of \mathbb{F}_q , the “puffing up” operation kills any additive structure that could lead to a bad list-recovery configuration.

Remark 1.5 (on the dependence of L on the various parameters). Recall that a code which is ε -close to capacity is said to achieve the Elias bound if $L = O(\ell/\varepsilon)$. Note that in both [Theorem 1.2](#) and [Theorem 1.3](#), the dependence of L on ε is as we would hope. However, the dependence on the other parameters (particularly ℓ and q) is exponentially worse than the $O(\ell)$ dependence. We leave it as a natural open problem to improve on this dependency.

Remark 1.6 (comparison to [ZP81]). As mentioned earlier, we are not aware of any prior arguments establishing non-trivial bounds on the list-size L for codes ε -close to capacity which do not require q to be large, other than what follows from the Zyablov–Pinsker argument [ZP81] (given formally in [Gur03]). Recall that this method guarantees list size $L = q^{O(\ell/\varepsilon)}$. In comparison, we obtain (roughly) $L = \frac{1}{\varepsilon} \cdot q^{O(\ell \log q)}$ in the case of erasures (over prime fields), and $L = \frac{1}{\varepsilon} \cdot q^{\ell \cdot \text{polylog}(q)}$ in the case of errors (over all fields, assuming ρ is not too close to 0 or $1 - \ell/q$). Thus, compared to [ZP81], we obtain a smaller bound on L once, roughly, $\varepsilon < \frac{1}{\text{polylog}(q)}$. In particular, when ℓ and q are constants we achieve asymptotic improvement in L .

1.2 Technical Overview

At a conceptual level, our work reconsiders the approach of Guruswami, Håstad, and Kopparty [GHK11], which allowed for an understanding of the list-decodability from errors of random linear codes over constant-sized alphabets, and adapts it to the case of list-recovery (either from erasures or errors). Recall that list-decoding from errors is the special case of list-recovery from errors with $\ell = 1$.

Using terminology that we define in this work, the first step in the argument of [GHK11] is to argue that Hamming balls are nontrivially *mixing*. Specifically, fix any center $z \in \mathbb{F}_q^n$ and consider sampling twice uniformly and independently from the Hamming ball of radius ρ centered at z ; denote the two samples by X and X' . The authors argue that for some $\delta > 0$ and any $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$, it follows that for any other center $y \in \mathbb{F}_q^n$, $\Pr[\alpha X + \beta X' \in B_\rho(y)] \leq q^{-\delta n}$ for

some $\delta = \delta(\rho, q) > 0$.³ Alternatively, we could say that for any $y \in \mathbb{F}_q^n$, we have $\Pr[\alpha X + \beta X' \in y + B_\rho(z)] \leq q^{-\delta n}$. From here, using some additional tools like *2-increasing chains* – whose existence they establish via a Ramsey-theoretic argument – they are able to show that random linear codes with ε gap-to-capacity are with high probability $(\rho, \frac{C(\rho, q)}{\varepsilon})$ -list-decodable from errors. In particular, their techniques promise the correct dependence on ε (although the dependence on the parameters q and ρ is quite poor).

We recommend viewing this “ δ -mixing” property in the following light. Any argument establishing that random linear codes have good list-decodability must somehow argue that random subspaces and Hamming balls don’t tend to “correlate” too much. In particular, it should not be the case that Hamming balls have noticeable “linear structure”, and in particular they should be “far” from being closed under addition.

In our work, we consider whether or not sets that are relevant for list-recovery, i.e., the sorts of sets that list-recoverable codes cannot intersect with too much, also have nontrivial mixing. Firstly, we crystallize in a definition what it means for any arbitrary set $T \subseteq \mathbb{F}_q^n$ to be δ -mixing, where $\delta > 0$: for any $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$ and $y \in \mathbb{F}_q^n$, if $X, X' \sim T$ – which denotes that X and X' are sampled independently and uniformly from T – then $\Pr[\alpha X + \beta X' \in y + T] \leq q^{-\delta n}$.

Now, for (α, ℓ, L) -list-recovery from erasures the relevant sets are combinatorial rectangles $T_1 \times T_2 \times \cdots \times T_n$ where for at least $(1 - \alpha)n$ values of $i \in [n]$ we have $|T_i| \leq \ell$. For (ρ, ℓ, L) -list-recovery from errors the sets are “puffed-up” combinatorial rectangles. Namely, for $T_1, T_2, \dots, T_n \subseteq \mathbb{F}_q$ each with $|T_i| \leq \ell$, we consider *list-recovery balls*

$$B_\rho(T_1 \times T_2 \times \cdots \times T_n) = \{x \in \mathbb{F}_q^n : x_i \notin T_i \text{ for at most } \rho n \text{ choices of } i \in [n]\}.$$

Following the argument of [GHK11], once we establish that these sets are nontrivially mixing, we can obtain bounds on the list-size with the correct dependence on ε . Our task then boils down to understanding the mixingness of the sets relevant for list-recovery. We consider first the erasures case, and subsequently discuss the errors case.

List-recovery from erasures Firstly, observe that for a combinatorial rectangle $T_1 \times \cdots \times T_n$, if each of the sets T_i is nontrivially mixing as a subset of \mathbb{F}_q (take the $n = 1$ case of the above definition), then $T_1 \times \cdots \times T_n$ is also nontrivially mixing (as a subset of \mathbb{F}_q^n). Hence, it suffices for us to consider whether or not subsets of \mathbb{F}_q mix. It is here that the dependence on the field size shows up.

Recall from the earlier discussion that [GLM⁺22] established that random linear codes over \mathbb{F}_{ℓ^t} (where ℓ is a prime power) are with high probability *not* (α, ℓ, L) -list-recoverable from erasures unless $L \geq \ell^{\Omega(1/\varepsilon)}$. Indeed, it is easy to find a subset $T \subseteq \mathbb{F}_{\ell^t}$ which is *not* δ -mixing for any $\delta > 0$: take $T = \mathbb{F}_\ell$ (or, more generally, any multiplicative coset $\gamma \cdot \mathbb{F}_\ell$ for $\gamma \in \mathbb{F}_{\ell^t} \setminus \{0\}$). Since \mathbb{F}_ℓ is closed under addition, in particular we have that if X and X' are sampled independently and uniformly from T then $\Pr[X + X' \in T] = 1$, so T is *not* δ -mixing for any $\delta > 0$.

What went wrong in this example? The fact that \mathbb{F}_{ℓ^t} contains \mathbb{F}_ℓ as a subfield means that \mathbb{F}_{ℓ^t} contains non-trivial \mathbb{F}_ℓ -linear subspaces. Such subspaces naturally create “bad” input lists, and the argument of [GLM⁺22] establishes that indeed a random linear code is likely to contain many vectors from a combinatorial rectangle $T_1 \times \cdots \times T_n$ where at least a $(1 - \alpha)$ fraction of the T_i ’s are 1-dimensional \mathbb{F}_ℓ -subspaces of \mathbb{F}_{ℓ^t} .

³In fact for [GHK11] it sufficed to only consider the $z = 0$ case, in which case one can always assume $\alpha = \beta = 1$. But their argument naturally generalizes to this case, and this is the notion of mixing that we require for our list-recovery results.

If we insist that q be a *prime*, then \mathbb{F}_q *does not* have any non-trivial subspaces. However, in this case \mathbb{F}_q still contains some subsets with “additive structure,” for example, taking ℓ to be odd here for simplicity, centered intervals⁴ like $I = \{-\frac{\ell-1}{2}, -\frac{\ell-1}{2} + 1, \dots, \frac{\ell-1}{2} - 1, \frac{\ell-1}{2}\} \subseteq \mathbb{F}_q$ have the property that if one samples $X, X' \sim I$ independently, then $\Pr[X + X' \in I] \approx \frac{3}{4} + \frac{1}{4\ell^2}$ assuming $\ell \leq 2q/3$. But note that this is still non-trivially bounded away from 1! Remarkably, an argument of Lev [Lev01] shows that this is the worst case over prime fields. More precisely, over all sets T of size ℓ , to maximize $\Pr[\alpha X + \beta X' \in \gamma + T]$ where $\alpha, \beta, \gamma \in \mathbb{F}_q$ with $\alpha, \beta \neq 0$, one should choose $T = I$ (the centered interval of length ℓ), $\alpha = \beta = 1$ and $\gamma = 0$. In our technical section we give an effective bound on $\Pr[X + X' \in I]$ for all $\ell < q$, which allows us to argue that combinatorial rectangles $T_1 \times \dots \times T_n$ in which at least a $1 - \alpha$ fraction of the T_i ’s have size at most ℓ are nontrivially mixing, as desired.

List-recovery from errors We now wish to establish that list-recovery balls are nontrivially mixing. Notably, unlike in the case of erasures, the argument here is *insensitive* to the base field. Let $T = T_1 \times \dots \times T_n$, where each $|T_i| \leq \ell$. Let $X, X' \sim B_\rho(T)$; in this overview, we will sketch how one bounds $\Pr[X + X' \in B_\rho(T)]$ (the argument easily generalizes to allow for multipliers $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$ and a shift $y \in \mathbb{F}_q^n$).

Unlike in the case of combinatorial rectangles, it is *not* the case that $X = (X_1, \dots, X_n)$ and $X' = (X'_1, \dots, X'_n)$ have independent coordinates. For example, conditioned on X_1 lying in T_1 , then X_2 is less likely to lie in T_2 . However, these correlations are relatively minor, and we can essentially “pretend” that both X and X' are sampled as follows: for each $i \in [n]$, with probability $1 - \rho$ set the i -th coordinate to a uniformly random element of T_i , and otherwise set it to a uniformly random element of $\mathbb{F}_q \setminus T_i$, and these choices are made independently for each $i \in [n]$.⁵ We remark that a similar trick is implicit in [GHK11], and made explicit in the context of rank-metric codes by Guruswami and Resch [GR18].

This new distribution is much more amenable to analysis. In particular, letting E_i be the indicator for the event $X_i + X'_i \in T_i$, then $X + X' \in B_\rho(T)$ iff $\sum_i E_i \geq (1 - \rho)n$. Thus, if we can argue $\Pr[E_i = 1] < 1 - \rho$ then a classic Chernoff-Hoeffding bound establishes $\Pr[\sum_i E_i \geq (1 - \rho)n]$ is exponentially small, implying the desired δ -mixing.

Bounding $\Pr[E_i = 1]$ is the most novel part of the analysis, and is done in Lemma 4.2. Recall that $X_i, X'_i \sim T_i$, and let also $Y_i, Y'_i \sim \mathbb{F}_q \setminus T_i$. We have

$$\begin{aligned} \Pr[E_i = 1] &= (1 - \rho)^2 \Pr[X_i + X'_i \in T_i] + 2\rho(1 - \rho) \Pr[X_i + Y'_i \in T_i] + \rho^2 \Pr[Y_i + Y'_i \in T_i] \\ &= \sum_{z_i \in T_i} (1 - \rho)^2 \Pr[X_i + X'_i = z_i] + 2\rho(1 - \rho) \Pr[X_i + Y'_i = z_i] + \rho^2 \Pr[Y_i + Y'_i = z_i] . \end{aligned} \quad (2)$$

As is standard, $\Pr[X_i + X'_i = z_i]$ is proportional to $1_{T_i} * 1_{T_i}(z_i)$, the convolution of the indicator functions for T_i , and similarly $\Pr[X_i + Y'_i = z_i]$ and $\Pr[Y_i + Y'_i = z_i]$ are proportional to $1_{T_i} * 1_{\mathbb{F}_q \setminus T_i}(z)$ and $1_{\mathbb{F}_q \setminus T_i} * 1_{\mathbb{F}_q \setminus T_i}(z)$, respectively. Using the simple identity $1_{\mathbb{F}_q \setminus T_i} = 1 - 1_{T_i}$, we can rewrite Equation (2) as

$$c \cdot 1_{T_i} * 1_{T_i}(z) + \text{other terms} ,$$

where c is a constant which we show to be positive assuming $\rho \in (0, 1 - \ell/q)$ (and indeed, if $\rho > 1 - \ell/q$ then it could be negative). Upon giving a trivial upper bound $1_{T_i} * 1_{T_i}(z_i)$ (which corresponds to

⁴Or, more generally, arithmetic progressions.

⁵In fact for technical reasons we have to consider X_i lying in T_i with probability ω for $\omega \leq \rho$, and similarly X'_i lies in T_i with probability $\omega' \leq \rho$. But by a concentration argument one can easily establish that ω and ω' are with high probability very close to ρ .

the case that T_i does not mix at all, as we must do since we are making no assumptions on the field) and simplifying, we obtain the bound

$$\Pr[E_i = 1] \leq (1 - \rho)^2 + \rho^2 \cdot \frac{\ell}{q - \ell}.$$

To our satisfaction, we have that $(1 - \rho)^2 + \rho^2 \cdot \frac{\ell}{q - \ell} < 1 - \rho$ iff $\rho \in (0, 1 - \ell/q)$, which is precisely the range of decoding radius at which we can hope for positive rate list-recovery from errors in the first place! Thus, we have that $\Pr[\sum_i E_i \geq (1 - \rho)n]$ is exponentially small, establishing that list-recovery balls nontrivially mix.

1.3 Open Problems

Lastly, we leave here some directions for future research:

- In our results the dependency on ε is correct, but the dependency on ℓ and q is rather poor. Can we improve this dependency? Or, can we perhaps prove new lower bounds on L in terms of ℓ and q that apply when these parameters are not too big?
- [GLM⁺22] showed that over \mathbb{F}_q with $q = \ell^t$ (and hence small characteristic), a random linear code is with high probability *not* (α, ℓ, L) -list-recoverable from erasures unless $L \geq \ell^{\Omega(1/\varepsilon)}$. Can we show that this lower bound actually applies to *every* q -ary linear code?
- Many arguments for codes being list-recoverable from errors in fact establish the stronger property of *average-radius-list-recovery*, where now one instead shows that for any input lists $T_1, \dots, T_n \subseteq \mathbb{F}_q$ of size ℓ , given $L + 1$ codewords $c^{(1)}, \dots, c^{(L+1)}$ one has

$$\frac{1}{L + 1} \sum_{j=1}^{L+1} 1_{\{c_i^{(j)} \notin T_i\}} > \rho n.$$

This in particular implies that there cannot be $L + 1$ codewords lying in a list-recovery ball of radius ρ . We believe our method should be able to establish this (slightly) stronger guarantee for random linear codes.

2 Preliminaries

2.1 Notation

We will often denote random variables and sets by uppercase Roman letters. The distinction will be clear from context. We write $[n] = \{1, \dots, n\}$ for any positive integer n . For a vector $v \in \mathbb{F}_q^n$ with \mathbb{F}_q the finite field of order q , we write $\text{Supp}(v) = \{i : v_i \neq 0\}$. We define the *weight* of v to be $\text{wt}(v) = |\text{Supp}(v)|$, and the *Hamming distance* between v and u is $d(u, v) = |\{i \in [n] : u_i \neq v_i\}| = |\text{Supp}(u - v)|$. For a collection of vectors $v_1, \dots, v_d \in \mathbb{F}_q^n$, we denote by $\text{Span}(v_1, \dots, v_d)$ the subspace of \mathbb{F}_q^n spanned by v_1, \dots, v_d .

We denote the *binary entropy function* by $h_2(\cdot)$, and recall that $h_2(x) = x \log_2 \frac{1}{x} + (1 - x) \log_2 \frac{1}{1 - x}$. For a positive integer q we shorthand $\exp_q(x) = q^x$. Additionally, by default \log is the base-2 logarithm. We write 1_A for the indicator function of a set A , and write $1_{\{E\}}$ for the indicator random variable that equals 1 if and only if the event E holds.

2.2 The Random Code Model

For an alphabet size q , a *plain random code* \mathcal{C} of block length n and rate $R \in [0, 1]$ is obtained by including each $x \in [q]^n$ in \mathcal{C} with probability $q^{-(1-R)n}$, and these choices are made independently for each x . (Note then that such a code has size q^{Rn} in expectation, and by a Chernoff bound it follows that it has rate $R \pm o(1)$ with high probability.)

When q is a prime power, a *random linear code* \mathcal{C} of block length n and rate $R \in [0, 1]$ is obtained by sampling a uniformly random matrix $H \in \mathbb{F}_q^{(1-R)n \times n}$, and defining

$$\mathcal{C} = \{x \in \mathbb{F}_q^n : Hx = 0\}.$$

Note that H is full-rank with probability $1 - O(q^{-Rn})$, and therefore \mathcal{C} has rate R with high probability.

Given any subset $S \subseteq [q]^n$, if \mathcal{C} is a plain random code of rate R then $\Pr[S \subseteq \mathcal{C}] = q^{-(1-R)n|S|}$. When dealing with random linear codes, the probability that a set appears in the code is determined by the span of the set.

Proposition 2.1. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a random linear code of block length n and rate $R \in [0, 1]$, and let $x_1, \dots, x_b \in \mathbb{F}_q^n$. Then,*

$$\Pr[\forall i \in [b], x_i \in \mathcal{C}] = q^{-(1-R)n \dim(\text{Span}(v_1, \dots, v_b))}.$$

2.3 List-Recovery Notions

This section collects the basic notions of list-recovery we study.

List-recovery from erasures. We begin with the relevant definition.

Definition 2.2 (list recovery from erasures). *Let $\mathcal{C} \subseteq [q]^n$ be a q -ary code of block-length n . For an erasure radius $\alpha \in [0, 1)$ and input list size $1 \leq \ell \leq q$, we say that \mathcal{C} is (α, ℓ, L) -list-recoverable from erasures if for every $T_1, \dots, T_n \subseteq [q]$ such that $|T_i| \leq \ell$ for at least $(1 - \alpha)n$ of the i -s and $T_i = [q]$ for the remaining, it holds that*

$$|\mathcal{C} \cap (T_1 \times \dots \times T_n)| \leq L.$$

That is, in any combinatorial rectangle of which at least $(1 - \alpha)n$ of its side-lengths are at most ℓ (and the remainder can be as large as q), there are at most L codewords.

We will also consider list-recovery from errors. The concept of a list-recovery ball – which generalizes that of a Hamming ball – will be useful.

Definition 2.3 (list-recovery ball). *Let $q \in \mathbb{N}$ and let $T_1, \dots, T_n \subseteq [q]$. The list-recovery ball of radius ρ centered at $T_1 \times \dots \times T_n$ is*

$$B_\rho(T_1 \times \dots \times T_n) = \{x \in [q]^n : d(x, T_1 \times \dots \times T_n) \leq \rho n\}.$$

Above, we have extended the Hamming metric by setting

$$d(x, T_1 \times \dots \times T_n) = |\{i \in [n] : x_i \notin T_i\}|.$$

We now state the relevant capacity theorem for list-recovery from erasures. The proofs of the two implications are standard: the *possibility* result follows from analyzing the performance of a plain random code, while the *impossibility* result follows from a counting argument.

Theorem 2.4 (list-recovery from erasures capacity). *Let $1 \leq \ell \leq q$ and let $\alpha \in [0, 1)$. Fix $\varepsilon > 0$. For $n \in \mathbb{N}$ large enough, the following hold:*

- *There exists a code $\mathcal{C} \subseteq [q]^n$ of rate $1 - (1 - \alpha) \log_q \ell - \alpha - \varepsilon$ which is $(\alpha, \ell, \lceil \ell/\varepsilon \rceil)$ -list-recoverable from erasures.*
- *For any code $\mathcal{C} \subseteq [q]^n$ of rate $1 - (1 - \alpha) \log_q \ell - \alpha + \varepsilon$, there exist $T_1, \dots, T_n \subseteq [q]$ with $|T_i| \leq \ell$ for at least $(1 - \alpha)n$ values of $i \in [n]$ such that $|\mathcal{C} \cap (T_1 \times \dots \times T_n)| \geq q^{\varepsilon n - o(n)}$.*

We therefore say that the *capacity* for (α, ℓ, L) -list-recovery from erasures is $1 - \alpha - (1 - \alpha) \log_q \ell$. We will study what happens for codes of rate $1 - (1 - \alpha) \log_q \ell - \alpha - \varepsilon$ for some $\varepsilon > 0$, and determine the value of their output list-size L . We will be focused on the case where q and ℓ is held constant, and the gap-to-capacity ε tends to 0.

List-recovery from errors. We now define what it means for a code to be list-recoverable from errors.

Definition 2.5 (list recovery from errors). *Let $\mathcal{C} \subseteq [q]^n$ be a q -ary code of block-length n . For a decoding radius $\rho \in (0, 1 - \ell/q)$ and input list size $1 \leq \ell \leq q$, we say that \mathcal{C} is (ρ, ℓ, L) -list-recoverable from errors if for every $T_1, \dots, T_n \subseteq [q]$ such that $|T_i| \leq \ell$ for all $i \in [n]$, it holds that*

$$|\mathcal{C} \cap B_\rho(T_1 \times \dots \times T_n)| \leq L.$$

That is, every list-recovery ball of radius ρ with side-lengths $\leq \ell$ contains at most L codewords.

We will need an estimate on the size of list-recovery balls. It makes use of the (q, ℓ) -entropy function, defined as follows:

$$h_{q,\ell}(x) = x \log_q \frac{q - \ell}{x} + (1 - x) \log_q \frac{q - \ell}{1 - x}. \quad (3)$$

An operational interpretation of this quantity is as the base- q entropy of a random variable which, with probability $1 - x$, samples a uniformly random element from a set of size ℓ , and with probability x samples a uniformly random element from the complement. Additionally, so long as $0 < x < 1 - \ell/q$ it holds that $0 < h_{q,\ell}(x) < 1$. Note that if $\ell = 1$ one recovers the q -entropy function, which we denote as h_q (i.e., if ℓ is omitted from the subscript, then it is by default 1).

We now state the relevant estimate.

Proposition 2.6 ([Res20, Proposition 2.4.11]). *Let $1 \leq \ell \leq q$ be integers and $\rho \in (0, 1 - \ell/q)$. Let $T_1, \dots, T_n \subseteq [q]$ with $|T_i| = \ell$ for all $i \in [n]$. Then,*

$$\frac{q^{nh_{q,\ell}(\rho)}}{\sqrt{2n}} \leq |B_\rho(T_1 \times \dots \times T_n)| \leq q^{nh_{q,\ell}(\rho)}.$$

Remark 2.7. In [Res20] the lower bound is just given as $q^{nh_{q,\ell}(\rho) - o(n)}$. Using an estimate of Wozencraft and Reiffen [WR61] (which we use below in the proof of [Proposition 2.14](#)), it follows that one can take the $q^{-o(n)}$ term to be $\frac{1}{\sqrt{2n}}$.

This estimate drives the following capacity theorem.

Theorem 2.8 (list-recovery from errors capacity). *Let $1 \leq \ell \leq q$ and let $\rho \in (0, 1 - \ell/q)$. Fix $\varepsilon > 0$. For $n \in \mathbb{N}$ large enough, the following hold:*

- There exists a code $\mathcal{C} \subseteq [q]^n$ of rate $1 - h_{q,\ell}(\rho) - \varepsilon$ which is $(\rho, \ell, \lceil \ell/\varepsilon \rceil)$ -list-recoverable from errors.
- For any code $\mathcal{C} \subseteq [q]^n$ of rate $1 - h_{q,\ell}(\rho) + \varepsilon$, there exists $T_1, \dots, T_n \subseteq [q]$ with $|T_i| \leq \ell$ for all $i \in [n]$ such that $|\mathcal{C} \cap B_\rho(T_1 \times \dots \times T_n)| \geq q^{\varepsilon n - o(n)}$.

Thus, we will concern ourselves with codes of rate $1 - h_{q,\ell}(\rho) - \varepsilon$, and determine the output list size L for (ρ, ℓ, L) -list-recovery from errors. And, as in the list-recovery from erasures case, we will hold ρ, ℓ, q constants and consider the asymptotic behaviour of L as the gap-to-capacity $\varepsilon \rightarrow 0$.

We will also need the following lower bound on the difference $h_{q,\ell}(\rho) - h_{q,\ell}(\rho - \eta)$.

Claim 2.9. *For any integers $q > 0$ and $1 \leq \ell \leq q$, any $\rho \in (0, 1 - \ell/q]$, and any $\eta \in [0, \rho]$, we have*

$$h_{q,\ell}(\rho) - h_{q,\ell}(\rho - \eta) \geq \eta \log_q \left(\frac{(q - \ell)(1 - \rho)}{\ell \cdot \rho} \right) \geq 0.$$

Proof. We can rewrite

$$h_{q,\ell}(\rho) - h_{q,\ell}(\rho - \eta) = \frac{h_2(\rho) - h_2(\rho - \eta)}{\log q} + \eta \log_q \left(\frac{q - \ell}{\ell} \right).$$

Now, the desired lower bound follows if we show that

$$h_2(\rho) - h_2(\rho - \eta) \geq \eta \log \left(\frac{1 - \rho}{\rho} \right)$$

for all $\rho \in [0, 1]$ and $\eta \in [0, \rho]$. To see this, first note that $h'_2(\rho) = \log \left(\frac{1 - \rho}{\rho} \right)$. Since h_2 is concave in $[0, 1]$, we have $h_2(\rho) - h_2(\rho - \eta) \geq \eta \cdot h'_2(\rho)$, as desired.

Finally, the rightmost lower bound “ ≥ 0 ” holds under the lemma’s hypotheses since $\frac{(q - \ell)(1 - \rho)}{\ell \cdot \rho} \geq 1$ if and only if $\rho \leq 1 - \ell/q$. \square

2.4 Some Distributions and Concentration Bounds

For a given finite set S in some universe U , we write $X \sim S$ to denote that X is distributed uniformly over the set S . For $p \in [0, 1]$, we denote by $\text{Ber}(p)$ the distribution of a Bernoulli random variable, which equals 1 with probability p and equals 0 with probability $1 - p$. By $\text{Bin}(n, p)$, we denote a binomial random variable which is the sum of n i.i.d. $\text{Ber}(p)$ random variables.

We now provide a tail bound on $\text{Bin}(n, p)$ random variables. It makes use of the concept of a Kullback–Leibler divergence between two Bernoulli random variables. Specifically, for $x, y \in [0, 1]$, define

$$D(x||y) = x \ln \frac{x}{y} + (1 - x) \ln \frac{1 - x}{1 - y}.$$

Proposition 2.10. *Let $X \sim \text{Bin}(n, p)$ with $0 < p < 1$, and let $p < p' < 1$. Then*

$$\Pr[X \geq p'n] \leq e^{-nD(p'||p)}.$$

As a very simple corollary, we note that if we define for $q \in \mathbb{N}$

$$D_q(x||y) = x \log_q \frac{x}{y} + (1 - x) \log_q \frac{1 - x}{1 - y},$$

then the following holds:

Corollary 2.11. *Let $X \sim \text{Bin}(n, p)$ with $0 < p < 1$, and let $p < p' < 1$. Then,*

$$\Pr[X \geq p'n] \leq q^{-nD_q(p'\|p)}.$$

We will make use of the following properties of KL divergence.

Claim 2.12. *Suppose $1 > p_1 > p_2 > p_3 > 0$. Then,*

$$D_q(p_1\|p_3) > D_q(p_1\|p_2) > 0.$$

Claim 2.13. *Let $p \in (0, 1)$ and $0 \leq \Delta < p$. Then,*

$$D(p\|p - \Delta) \geq 2\Delta^2.$$

Additionally, we need to lower bound the probability that a binomial random variable hits exactly its expectation.

Proposition 2.14. *Let $X \sim \text{Bin}(n, p)$ with $0 < p < 1$ such that pn is an integer. Then,*

$$\Pr[X = pn] \geq \frac{1}{\sqrt{2n}}.$$

Proof. First, note that

$$\Pr[X = pn] = \binom{n}{pn} p^{pn} (1-p)^{(1-p)n} = \binom{n}{pn} \cdot 2^{-nh_2(p)},$$

The desired statement follows by combining this observation with a bound of Wozencraft and Reiffen [WR61] (see [CT06, Lemma 17.5.1]), which in particular gives that

$$\binom{n}{pn} \cdot 2^{-nh_2(p)} \geq \frac{1}{\sqrt{8p(1-p)n}} \geq \frac{1}{\sqrt{2n}}. \quad \square$$

2.5 Increasing Chains

The following definition of an increasing chain was first introduced by Guruswami, Håstad, and Kopparty [GHK11].

Definition 2.15 (*c*-increasing chain). *A sequence of vectors $v_1, \dots, v_d \subseteq \mathbb{F}_q$ is said to be a *c*-increasing chain of length d if for all $j \in [d]$ we have*

$$\left| \text{Supp}(v_j) \setminus \left(\bigcup_{i=1}^{j-1} \text{Supp}(v_i) \right) \right| \geq c.$$

We require the following lemma on the existence of appropriately long increasing chains in any subset $S \subseteq \mathbb{F}_q$.

Lemma 2.16 ([GHK11, Lemma 6.3]). *For every prime power q , and all positive integers c, ℓ and $L \leq q^\ell$, the following holds. For every $S \subseteq \mathbb{F}_q^\ell$ with $|S| = L$, there is $w \in \mathbb{F}_q^\ell$ such that $S + w$ has a *c*-increasing chain of length at least $\frac{1}{c} \log_q \frac{L}{2} - (1 - \frac{1}{c}) \log_q ((q-1)\ell)$.*

2.6 Mixing Sets

In our analysis we need to understand the probability that the sum of two independent uniformly random samples X and X' from a set $T \subseteq \mathbb{F}_q$ lands in a shifted set $T + \gamma$, for an arbitrary shift $\gamma \in \mathbb{F}_q$ (and in fact a more general question of that form). We begin with the necessary definitions.

Definition 2.17 (mixing over \mathbb{F}_q). *For a prime power q , and $\delta \geq 0$, we say that $T \subseteq \mathbb{F}_q$ is δ -mixing, if for any $\alpha, \beta, \gamma \in \mathbb{F}_q$, where α and β are nonzero, it holds that*

$$\Pr_{X, X'}[\alpha X + \beta X' \in T + \gamma] \leq q^{-\delta},$$

where $X, X' \sim T$ are independent and uniformly distributed over T , and $T + \gamma = \{t + \gamma : t \in T\}$.

Definition 2.18 (mixing over \mathbb{F}_q^n). *For $n \in \mathbb{N}$, a prime power q , and $\delta \geq 0$, we say that $T \subseteq \mathbb{F}_q^n$ is δ -mixing, if for any nonzero $\alpha, \beta \in \mathbb{F}_q$, and any $z \in \mathbb{F}_q^n$, it holds that*

$$\Pr_{X, X'}[\alpha X + \beta X' \in T + z] \leq q^{-\delta n},$$

where $X, X' \sim T$ are independent and uniformly distributed over T .

Remark 2.19. Note that a set mixes nontrivially when $\delta > 0$, and moreover, we will want $\delta > 0$ to not depend on n . However, in the case of list recovery from erasures, where for some i -s, $S_i = \mathbb{F}_q$, the case of $\delta = 0$ will be useful towards bounding the *expected* mixing of S_1, \dots, S_n .

The following connection then follows easily.

Remark 2.20. Suppose that $T_1, \dots, T_n \subseteq \mathbb{F}_q$, and each T_i is δ_i -mixing. Then, $T = T_1 \times \dots \times T_n$ is δ -mixing, for $\delta = \mathbb{E}_{i \sim [n]}[\delta_i]$.

3 List-Recovery from Erasures over Prime Fields

In this section we establish the list-recoverability of random linear codes over prime fields. To achieve this, we must first understand the mixing properties of worst-case subsets of prime fields.

3.1 Worst-Case Mixing of Subsets of Prime Fields

Towards understanding mixing of subsets of prime fields, we leverage a general result of Lev [Lev01] which characterizes worst-case T -s, when q is prime. Before we introduce it, we set up some relevant notation.

For a set $T \subseteq \mathbb{F}_q$ we let \tilde{T} denote a “centered interval” of length $|T|$. More precisely, \tilde{T} is the δ -centered interval associated with T if $\tilde{T} = [-\alpha, \alpha + \delta] \subseteq \mathbb{F}_q$ with $\alpha \in [0, \frac{q-1}{2}]$ and $\delta \in \{-1, 0, 1\}$ satisfying $|\tilde{T}| = 2\alpha + 1 + \delta = |T|$. Note that when $|T|$ is odd there is a unique centered interval \tilde{T} (because $\delta = 0$ necessarily), but when $|T|$ is even there are two centered intervals, corresponding to $\delta = \pm 1$.

Lemma 3.1 ([Lev01, Theorem 1], adapted). *Let $q \geq 3$ be prime and $A_1, \dots, A_k \subseteq \mathbb{F}_q$ be arbitrary sets with $\tilde{A}_1, \dots, \tilde{A}_k$ the associated δ_i -centered intervals. Then, if $|\delta_1 + \dots + \delta_k| \leq 1$, for any set $B \subseteq \mathbb{F}_q$ and some associated δ -centered interval \tilde{B} , we have*

$$\Pr_{X_i \sim A_i}[X_1 + \dots + X_k \in B] \leq \Pr_{\tilde{X}_i \sim \tilde{A}_i}[\tilde{X}_1 + \dots + \tilde{X}_k \in \tilde{B}].$$

We can use [Lemma 3.1](#) to prove the following.

Lemma 3.2. *Fix a prime $q \geq 3$. Let $T_1, T_2, T_3 \subseteq \mathbb{F}_q$ be arbitrary sets of size $\ell > 0$. Then,*

$$\Pr_{X_1 \sim T_1, X_2 \sim T_2} [X_1 + X_2 \in T_3] \leq \begin{cases} \frac{3}{4} + \frac{1}{4\ell^2} + \frac{\max(0, 3\ell-2q-1) \cdot (3\ell-2q+1)}{4\ell^2}, & \text{if } \ell \text{ is odd,} \\ \frac{3}{4} + \frac{\max(0, 3\ell-2q)^2}{4\ell^2}, & \text{if } \ell \text{ is even,} \end{cases}$$

and this is tight for all ℓ . In particular:

1. When $\ell \leq 2q/3$ we have

$$\Pr_{X_1 \sim T_1, X_2 \sim T_2} [X_1 + X_2 \in T_3] \leq \begin{cases} \frac{3}{4} + \frac{1}{4\ell^2}, & \text{if } \ell \text{ is odd,} \\ \frac{3}{4}, & \text{if } \ell \text{ is even.} \end{cases}$$

2. When $2q/3 < \ell \leq q-1$ we have

$$\Pr_{X_1 \sim T_1, X_2 \sim T_2} [X_1 + X_2 \in T_3] \leq \frac{q^2 - 3\ell(q - \ell)}{\ell^2}.$$

Proof. By [Lemma 3.1](#), we have

$$\Pr_{X_1 \sim T_1, X_2 \sim T_2} [X_1 + X_2 \in T_3] \leq \Pr_{\tilde{X}_1 \sim \tilde{T}_1, \tilde{X}_2 \sim \tilde{T}_2} [\tilde{X}_1 + \tilde{X}_2 \in \tilde{T}_3],$$

where $\tilde{T}_1, \tilde{T}_2, \tilde{T}_3$ are (possibly different) centered intervals associated with T_1, T_2, T_3 , respectively. We consider two cases depending on the parity of ℓ .

If ℓ is odd, then $\tilde{T}_1 = \tilde{T}_2 = \tilde{T}_3 = [-\alpha, \alpha]$ with $\alpha = \frac{\ell-1}{2}$. Therefore,

$$\begin{aligned} \Pr_{X_1 \sim T_1, X_2 \sim T_2} [X_1 + X_2 \in T_3] &\leq \Pr_{\tilde{X}_1, \tilde{X}_2 \sim [-\alpha, \alpha]} [\tilde{X}_1 + \tilde{X}_2 \in [-\alpha, \alpha]] \\ &= \sum_{i=-\alpha}^{\alpha} \sum_{j=-\alpha}^{\alpha} \frac{1}{\ell^2} \cdot 1_{\{i+j \pmod q \in [-\alpha, \alpha]\}}, \end{aligned}$$

where we interpret the mod q operation as mapping to $[-\frac{q-1}{2}, \frac{q-1}{2}]$. The term inside the double sum is 1 exactly when one of the following three disjoint cases occurs:

- $i + j \in [-\alpha, \alpha]$: By symmetry we can focus on $i \geq 0$, in which case this is equivalent to $j \in [-\alpha, \alpha - i]$. Therefore, the probability that this event occurs is (recall that $\ell = 2\alpha + 1$)

$$\frac{1}{\ell} + \frac{2}{\ell^2} \sum_{i=1}^{\alpha} ((\alpha - i) - (-\alpha) + 1) = \frac{1}{\ell} + \frac{2}{\ell^2} \sum_{i=1}^{\alpha} (\ell - i) = \frac{3}{4} + \frac{1}{4\ell^2}.$$

The factor of 2 comes from grouping together $\pm i$ for $i > 0$ by symmetry. The leftmost $\frac{1}{\ell}$ term corresponds to $i = 0$.

- $i + j \in [q - \alpha, q]$: This is equivalent to $j \in [q - \alpha - i, \alpha]$, because $i + j \in [q - \alpha, q]$ is equivalent to $j \in [q - \alpha - i, q - i]$. We also know that $j \in [-\alpha, \alpha]$. Since $q - i \geq \alpha$ for all $i \leq \alpha$ (because $\alpha \leq \frac{q-1}{2}$), the intersection of the two intervals is $[q - \alpha - i, \alpha]$. Note that the interval

$[q - \alpha - i, \alpha]$ is non-empty if and only if $i \geq q - 2\alpha = q - \ell$. Therefore, the probability of this case occurring is

$$\frac{1}{\ell^2} \sum_{i=q-\ell}^{\alpha} (\alpha - (q - \alpha - i) + 1) = \frac{1}{\ell^2} \sum_{i=q-\ell}^{\alpha} (\ell - q + i).$$

This sum is nonzero only when $\alpha > q - \ell$, which is equivalent to $3\ell - 2q - 1 > 0$. Therefore, this expression simplifies to

$$\frac{\max(0, 3\ell - 2q - 1) \cdot (3\ell - 2q + 1)}{8\ell^2}.$$

- $i + j \in [-q, -q + \alpha]$: By symmetry, the probability that this case occurs is equal to the previous case.

Summing the three probabilities yields the desired result for odd ℓ -s.

If ℓ is even, we can choose the centered intervals $\tilde{T}_1 = [-\alpha, \alpha - 1]$ and $\tilde{T}_2 = [-\alpha + 1, \alpha]$ for $\alpha = \ell/2$. The δ_3 -centered interval \tilde{T}_3 associated with T_3 also must have $\delta_3 = \pm 1$. Without loss of generality we assume that $\tilde{T}_3 = \tilde{T}_2 = [-\alpha + 1, \alpha]$ (otherwise, flip α to $-\alpha$). Now,

$$\begin{aligned} \Pr_{X_1 \sim \tilde{T}_1, X_2 \sim \tilde{T}_2} [X_1 + X_2 \in T_3] &\leq \Pr_{\tilde{X}_1 \sim [-\alpha, \alpha - 1], \tilde{X}_2 \sim [-\alpha + 1, \alpha]} [\tilde{X}_1 + \tilde{X}_2 \in [-\alpha + 1, \alpha]] \\ &= \frac{1}{\ell^2} \sum_{i=-\alpha}^{\alpha-1} \sum_{j=-\alpha+1}^{\alpha} 1_{\{i+j \pmod{q} \in [-\alpha+1, \alpha]\}}, \end{aligned}$$

where, as before, we interpret the mod q operation as mapping to $[-\frac{q-1}{2}, \frac{q-1}{2}]$. The term inside the double sum is 1 exactly when one of the following three disjoint cases occurs:

- $i + j \in [-\alpha + 1, \alpha]$: This is equivalent to $j \in [-\alpha + 1, \alpha - i]$ if $i \geq 0$ and to $j \in [-\alpha + 1 - i, \alpha]$ if $i < 0$. Therefore, the probability of this case occurring is (recall that $\ell = 2\alpha$)

$$\begin{aligned} &\frac{1}{\ell^2} \sum_{i=0}^{\alpha-1} (\alpha - i - (-\alpha + 1) + 1) + \frac{1}{\ell^2} \sum_{i=-\alpha}^{-1} (\alpha - (-\alpha + 1 - i) + 1) \\ &= \frac{1}{\ell^2} \sum_{i=0}^{\alpha-1} (\ell - i) + \frac{1}{\ell^2} \sum_{i=-\alpha}^{-1} (\ell + i) = \frac{3}{4}. \end{aligned}$$

- $i + j \in [q - \alpha + 1, q]$: This is equivalent to $j \in [q - \alpha + 1 - i, \alpha]$. Therefore, the probability of this case occurring is

$$\frac{1}{\ell^2} \sum_{i=-\alpha}^{\alpha-1} \max(0, (\alpha - (q - \alpha + 1 - i) + 1)) = \frac{1}{\ell^2} \sum_{i=-\alpha}^{\alpha-1} \max(0, \ell - q + i) = \frac{1}{\ell^2} \sum_{i=q-\ell}^{\alpha-1} (\ell - q + i).$$

The rightmost sum is positive only if $\alpha - 1 \geq q - \ell$, which is equivalent to $3\alpha - q > 0$. Therefore, we can simplify that right-hand side as

$$\frac{\max(0, 3\alpha - q) \cdot (3\alpha - q - 1)}{2\ell^2} = \frac{\max(0, 3\ell - 2q) \cdot (3\ell - 2q - 2)}{8\ell^2}.$$

- $i + j \in [-q, -q + \alpha]$: This is equivalent to $j \in [-\alpha + 1, -q + \alpha - i]$. Therefore, the probability of this case occurring is

$$\frac{1}{\ell^2} \sum_{i=-\alpha}^{\alpha-1} \max(0, -q + \alpha - i - (-\alpha + 1) + 1) = \frac{1}{\ell^2} \sum_{i=-\alpha}^{\alpha-1} \max(0, \ell - q - i) = \frac{1}{\ell^2} \sum_{i=-\alpha}^{\ell-q} (\ell - q - i).$$

The rightmost sum is positive only if $3\alpha - q > 0$, and so we can simplify the right-hand side as

$$\frac{\max(0, 3\alpha - q) \cdot (3\alpha - q + 1)}{2\ell^2} = \frac{\max(0, 3\ell - 2q) \cdot (3\ell - 2q + 2)}{8\ell^2}.$$

Summing the probabilities for the three cases yields the desired result for even ℓ -s.

Regarding the “In particular” part, **Item 1** follows directly by noticing that all maximums are 0 when $\ell \leq 2q/3$. **Item 2** uses the fact that when $\ell > 2q/3$ both upper bounds (for even and odd ℓ) simplify to $\frac{q^2 - 3\ell(q - \ell)}{\ell^2}$. \square

We can then record the following corollary.

Corollary 3.3. *For a prime $q \geq 3$, any set $T \subseteq \mathbb{F}_q$ of size $\ell \leq q - 1$,*

- *If $2 \leq \ell \leq 2q/3$, T is δ -mixing for $\delta \geq \log_q(16/13)$.*
- *Otherwise, T is δ -mixing for $\delta \geq \log_q\left(\frac{\ell^2}{q^2 - 3\ell(q - \ell)}\right)$.*

3.2 List-Recovery from Erasures over Prime Fields via Mixing

In this section we adapt the technique in [GHK11], together with the worst-case mixing result from **Corollary 3.3**, to establish list recovery from erasures over prime fields.

Lemma 3.4. *Let $T \subseteq \mathbb{F}_q^n$ be δ -mixing. For $b \in \mathbb{N}$ and any $a > 0$ satisfying $n \geq q^{\frac{8a}{\delta}}$, the following holds. Let $X^{(1)}, \dots, X^{(b)}$ be sampled independently and uniformly at random from T . Then, we have that*

$$\Pr\left[|\text{Span}(X^{(1)}, \dots, X^{(b)}) \cap T| > C \cdot b\right] \leq q^{-an},$$

where $C = C(q, \delta, a) = q^{\frac{8a}{\delta}}$. In particular, when $T = T_1 \times \dots \times T_n$, and each T_i is δ_i -mixing, we get the same result as above for $\delta = \mathbb{E}_i[\delta_i]$.

Proof. Let E denote the bad event that we want to bound, namely $|\text{Span}(X^{(1)}, \dots, X^{(b)}) \cap T| > A$ for $A = b \cdot q^{\frac{8a}{\delta}}$. Note that E implies that there exists some set $S \subseteq \mathbb{F}_q^b$, $|S| = A + 1$, such that $X_v \triangleq \sum_{i \in [b]} v_i X^{(i)} \in T$ for all $v \in S$.⁶ Hence, it suffices to bound the probability that such a set S exists.

Fix some $S \subseteq \mathbb{F}_q^b$ of size $A + 1$. Applying **Lemma 2.16** with $c = 2$ (and note that we can assume that $A + 1 \leq q^b$), we know there exists $w \in \mathbb{F}_q^b$ such that $S + w$ has a 2-increasing chain of length $d = \frac{1}{2} \log_q \frac{A+1}{2} - \frac{1}{2} \log_q((q-1)b)$. That is, we have $v^{(1)}, \dots, v^{(d)} \in S$ such that for all $j \in [d]$,

$$\left| \text{Supp}(v^{(j)}) \setminus \left(\bigcup_{i=1}^{j-1} \text{Supp}(v^{(i)}) \right) \right| \geq 2.$$

⁶Notice that if the X_i -s are not linearly independent, this can only decrease the probability that the intersection is large, so we can concentrate on the case that distinct v -s give rise to distinct X_v -s.

Now, we can bound

$$\begin{aligned}
\Pr[\forall v \in S, X_v \in T] &\leq \Pr[\forall j \in [d], X_{v(j)} \in T] \\
&= \Pr[\forall j \in [d], X_{v(j)} + X_w \in T + X_w] \\
&= \Pr[\forall j \in [d], X_{v(j)+w} \in T + X_w].
\end{aligned} \tag{4}$$

Next, we bound Equation (4) by

$$\sum_{y \in \mathbb{F}_q^n} \Pr[\forall j \in [d], X_{v(j)+w} \in T + y]. \tag{5}$$

Towards bounding each term in the sum, observe that the increasing chain property tells us that for each $j \in [d]$, we can write $X_{v(j)+w} = Y_{\text{past}}^{(j)} + Y_{\text{new}}^{(j)}$, where $Y_{\text{past}}^{(j)}$ contains X_k -s that participated in $\{X_{v(i)+w}\}_{i < j}$, whereas $Y_{\text{new}}^{(j)}$ contains two new X_k -s. Now,

$$\Pr[X_{v(j)+w} \in T + y \mid \forall i \in [j-1], X_{v(i)+w} \in T + y] = \mathbb{E}_{z \sim Y_{\text{past}}^{(j)}} [\mathbf{1}(z) \cdot \Pr[Y_{\text{new}}^{(j)} \in T + y_z]], \tag{6}$$

where $\mathbf{1}(z)$ is an indicator for whether past X_k -s landed in $T + y$, and y_z is a fixed string that depends on the fixing of $Y_{\text{past}}^{(j)}$. Assume for simplicity that $Y_{\text{new}}^{(j)} = \alpha X^{(1)} + \beta X^{(2)}$, where $\alpha, \beta \in \mathbb{F}_q$ are nonzero. Then, using the fact that T is δ -mixing, each summand of Equation (5) can now be bounded by

$$\prod_{j \in [d]} \Pr[X_{v(j)+w} \in T + y \mid \forall i \in [j-1], X_{v(i)+w} \in T + y] \leq q^{-n\delta d},$$

and summing over all y -s gives us

$$\Pr[v \in S, X_v \in T] \leq q^n \cdot q^{-n\delta d} = q^{-(\delta d - 1)n}.$$

Union-bounding over all S -s, we get

$$\Pr[E] \leq \binom{q^b}{A+1} q^{-(\delta d - 1)n} \leq q^{b(A+1) - (\delta d - 1)n}. \tag{7}$$

First, note that we set parameters so that $d \geq \frac{2a+1}{\delta}$. Indeed, we can set $d = \left\lfloor \frac{1}{2} \log_q \left(\frac{A+1}{2b(q-1)} \right) \right\rfloor$, and then need A to be at most, say, $4q \cdot q^{\frac{4a}{\delta}} \leq q^{\frac{8a}{\delta}}$. Under this choice of A , it also holds that $b(A+1) \leq \frac{\delta d - 1}{2}n$, since n is large enough. Overall, Equation (7) gives $\Pr[E] \leq q^{-\frac{\delta d - 1}{2}n} \leq q^{-an}$, as desired. The ‘‘In particular’’ part simply follows from Remark 2.20. \square

We are now ready to prove our list recovery result.

Theorem 3.5 (list recovery with erasures). *For any $n \in \mathbb{N}$, a prime q , an integer $\ell \leq q - 1$, and $\alpha, \varepsilon \in (0, 1)$, the following holds. With probability at least $1 - q^{-n}$, a random linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of rate*

$$R = 1 - \alpha - (1 - \alpha) \log_q \ell - \varepsilon$$

is (α, ℓ, L) -list-recoverable from erasures, with

$$L = C_{q, \ell, \alpha} \cdot \frac{1}{\varepsilon},$$

provided that $n \geq L$. In particular, there exists a universal constant C such that:

- When $\ell \leq \frac{2}{3}q$, we can take $C_{q,\ell,\alpha} \leq q^{C \log q \cdot ((1-\alpha)\ell+1)} \triangleq C_{q,\ell,\alpha}^{(0)}$, and,
- When $\ell = (1-\gamma)q$ for some $\gamma \in (0, 1/3)$, we can take $C_{q,\ell,\alpha} \leq \left(C_{q,\ell,\alpha}^{(0)}\right)^{\frac{(1-\gamma)^2}{1-3\gamma(1-\gamma)}}$.

Proof. Fix some $T_1, \dots, T_n \subseteq \mathbb{F}_q$, and some set $\mathbf{B} \subseteq [n]$ of density α , such that for all $i \notin \mathbf{B}$, $|T_i| \leq \ell$, and otherwise $T_i = \mathbb{F}_q$. Denote $T = T_1 \times \dots \times T_n$, and record that there are

$$\mathcal{T} \leq \binom{n}{\alpha n} \binom{q}{\ell}^{(1-\alpha)n} \leq 2^{h_2(\alpha)n} \cdot \left(\frac{eq}{\ell}\right)^{(1-\alpha)n\ell} = q^{\frac{h_2(\alpha)}{\log q}n + (1-\alpha)n\ell}$$

options to choose such a T .

For each $b \in [\log_q(L+1), L+1]$, let \mathcal{F}_b be the set of all $(v_1, \dots, v_b) \in T^b$ such that the v_i -s are linearly independent, and $|\text{Span}(\{v_1, \dots, v_b\}) \cap T| > L$. Further, let $\mathcal{F} = \bigcup_b \mathcal{F}_b$. Given a tuple $\mathbf{v} = (v_1, \dots, v_b)$, we denote by $\{\mathbf{v}\}$ the (unordered) set $\{v_1, \dots, v_b\}$.

Note that if $|T \cap \mathcal{C}| > L$, there must exist some $\mathbf{v} \in \mathcal{F}$ for which $\{\mathbf{v}\} \subseteq T \cap \mathcal{C}$, by taking a maximal linearly independent subset of $T \cap \mathcal{C}$. Now, for some fixed $\mathbf{v} \in \mathcal{F}_b$,

$$\Pr_{\mathcal{C}}[\mathbf{v} \subseteq T \cap \mathcal{C}] \leq \Pr_{\mathcal{C}}[\mathbf{v} \subseteq \mathcal{C}] \leq q^{-(1-R)nb},$$

where we used [Proposition 2.1](#). Overall, to bound the probability p that the code is not list-recoverable, we need to union-bound over the choice of T , and over the $\{\mathbf{v}\}$ -s. Concretely,

$$p \leq \mathcal{T} \cdot \sum_{b \in [\log_q(L+1), L+1]} \sum_{\mathbf{v} \in \mathcal{F}_b} q^{-(1-R)nb}. \quad (8)$$

We break the above sum with respect to a threshold $b^* = \lceil c \cdot \frac{\ell}{\varepsilon} \rceil$, for c to be determined soon. When $b < b^*$, we apply [Lemma 3.4](#) as follows. The parameter a will be determined later on. To determined δ , note that whenever $T_i = \mathbb{F}_q$, T_i is trivially 0-mixing, whereas for $|T_i| = \ell$, T_i is δ_i -mixing for either $\delta_0 \geq \log_q(16/13)$, or $\delta_0 \geq \log_q\left(\frac{\ell^2}{q^2 - 3\ell(q-\ell)}\right)$, following [Corollary 3.3](#). Thus, $\delta \geq (1-\alpha)\delta_0$, and we will set a and c so that $L \geq q^{\frac{8a}{\delta}} \cdot \frac{c\ell}{\varepsilon}$. Using our terminology, [Lemma 3.4](#) tells us that

$$\Pr_{\mathbf{v} \sim T^b} [|\text{Span}(\{\mathbf{v}\}) \cap T| > L] \leq q^{-an},$$

so in particular, $|\mathcal{F}_b| \leq |T|^b \cdot q^{-an}$, and we can bound

$$\begin{aligned} p_1 &\triangleq \mathcal{T} \sum_{b=\log_q(L+1)}^{b^*} \sum_{\mathbf{v} \in \mathcal{F}_b} q^{-(1-R)nb} \leq \mathcal{T} \cdot b^* \cdot q^{-an} \cdot \sum_{b=\log_q(L+1)}^{b^*} |T|^b \cdot q^{-(1-R)nb} \\ &\leq \mathcal{T} \cdot b^* q^{-an} \sum_{b=\log_q(L+1)}^{b^*} q^{\alpha nb} \ell^{(1-\alpha)nb} q^{-(1-R)nb} = \mathcal{T} \cdot b^* q^{-an} \sum_{b=\log_q(L+1)}^{b^*} q^{-(1-R-\alpha-(1-\alpha)\log_q \ell)nb} \\ &\leq \mathcal{T} \cdot (b^*)^2 q^{-an} q^{-\varepsilon \cdot n \cdot \log_q(L+1)} \leq q^{\frac{h_2(\alpha)}{\log q}n + (1-\alpha)n\ell + 2\log b^* - an - \varepsilon n \cdot \log_q(L+1)} \\ &\leq q^{(1+(1-\alpha)\ell - a - \varepsilon \log_q(L+1))n}, \end{aligned}$$

where we used the fact that $\frac{h_2(\alpha)}{\log q} + \frac{2\log b^*}{n} \leq 1$. Now, $L+1 \geq q$, so it suffices to choose $a \geq (1-\alpha)\ell + 3$ to get that $p_1 \leq q^{-2n}$.

Moving on to p_2 , we have

$$p_2 \triangleq \mathcal{T} \sum_{b=b^*+1}^{L+1} \sum_{\mathbf{v} \in \mathcal{F}_b} q^{-(1-R)nb} \leq \mathcal{T} \cdot \sum_{b=b^*+1}^{L+1} |T|^b q^{-(1-R)nb} \leq \mathcal{T} \cdot \sum_{b=b^*+1}^{L+1} q^{-(1-R-\alpha-(1-\alpha)\log_q \ell)nb},$$

where we used the trivial bound on $|\mathcal{F}_b|$. Now,

$$p_2 \leq \mathcal{T} \cdot (L+1) \cdot q^{-\varepsilon nb^*} \leq q^{\frac{h_2(\alpha)}{\log q} n + (1-\alpha)n\ell + \log_q(L+1) - cn\ell} \leq q^{(2+(1-\alpha-c)\ell)n}.$$

Thus, choosing $c \geq 1 - \alpha + \frac{4}{\ell}$, we get that $p_2 \leq q^{-2n}$, and recalling Equation (8), we get that overall, $p \leq q^{-n}$. Finally, recall that the bound on p was provided that a and c are such that $L \geq q^{\frac{8a}{\delta}} \cdot \frac{c\ell}{\varepsilon}$. Indeed, if we set $a = (1-\alpha)\ell + 3$ and $c = 5$, this holds by choosing the constant C in the theorem's statement appropriately. \square

4 List-Recovery from Errors over Arbitrary Fields

We now turn to the case of list-recovery from errors. Unlike in the case of list-recovery from erasures, we will make no assumptions on the underlying field. We firstly show that list-recovery balls are non-trivially mixing. We subsequently sketch how, again using Lemma 3.2, we can conclude the desired list-recovery result.

4.1 Mixture of List-Recovery Balls

In this section we make use of the *convolution* of two functions $f, g: \mathbb{F}_q \rightarrow \mathbb{R}$, defined as

$$(f * g)(x) = \mathbb{E}_{y \in \mathbb{F}_q} [f(y)g(x-y)].$$

We recall that it is *distributive*, i.e., $f * (g + h) = f * g + f * h$ for any functions $f, g, h: \mathbb{F}_q \rightarrow \mathbb{R}$. We also note the following equality.

Proposition 4.1. *Let q be a prime power. Suppose $A, B \subseteq \mathbb{F}_q$ and X, Y are sampled independently and uniformly from A, B , respectively. Then, for any $z \in \mathbb{F}_q$,*

$$\Pr[X + Y = z] = \frac{q}{|A| \cdot |B|} 1_A * 1_B(z).$$

Proof. We have

$$\begin{aligned} \Pr[X + Y = z] &= \sum_{x \in A} \Pr[X = x] \Pr[X + Y = z | X = x] = \sum_{x \in A} \frac{1}{|A|} \cdot \Pr[Y = z - x] \\ &= \frac{1}{|A|} \sum_{x \in \mathbb{F}_q} 1_A(x) \cdot 1_B(z - x) \frac{1}{|B|} = \frac{q}{|A| \cdot |B|} \mathbb{E}_{x \in \mathbb{F}_q} [1_A(x) \cdot 1_B(z - x)] \\ &= \frac{q}{|A| \cdot |B|} 1_A * 1_B(z). \end{aligned} \quad \square$$

Lemma 4.2. *Suppose q is a prime power, $1 \leq \ell \leq q$ is an integer and $\omega_1, \omega_2 \in (0, 1 - \ell/q)$. Let $A, B, T \subseteq \mathbb{F}_q$ be of size ℓ , let $X_1 \sim \text{Unif}(A)$, $X_2 \sim \text{Unif}(B)$, $Y_1 \sim \text{Unif}(\mathbb{F}_q \setminus A)$ and $Y_2 \sim \text{Unif}(\mathbb{F}_q \setminus B)$ all independent. Then,*

$$(1 - \omega_1)(1 - \omega_2) \Pr[X_1 + X_2 \in T] + \omega_1(1 - \omega_2) \Pr[X_1 + Y_2 \in T] \quad (9)$$

$$\begin{aligned}
& + \omega_2(1 - \omega_1) \Pr[Y_1 + X_2 \in T] + \omega_1\omega_2 \Pr[Y_1 + Y_2 \in T] \\
& \leq (1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell} .
\end{aligned} \tag{10}$$

Proof. Using [Proposition 4.1](#) and the observation that $1_{\mathbb{F}_q \setminus A} = 1 - 1_A$ (and similarly for B), for any $z \in T$ we find

$$\begin{aligned}
\Pr[X_1 + X_2 = z] &= \frac{q}{\ell^2} \cdot 1_A * 1_B(z) , \\
\Pr[X_1 + Y_2 = z] &= \frac{q}{\ell(q - \ell)} \cdot 1_A * (1 - 1_B)(z) = \frac{q}{\ell(q - \ell)} \cdot \left(\frac{\ell}{q} - 1_A * 1_B(z) \right) , \\
\Pr[X_2 + Y_1 = z] &= \frac{q}{\ell(q - \ell)} \cdot (1 - 1_A) * 1_B(z) = \frac{q}{\ell(q - \ell)} \cdot \left(\frac{\ell}{q} - 1_A * 1_B(z) \right) \\
\Pr[Y_1 + Y_2 = z] &= \frac{q}{(q - \ell)^2} \cdot (1 - 1_A) * (1 - 1_B)(z) \\
&= \frac{q}{(q - \ell)^2} \cdot \left(1 - 2 \cdot \frac{\ell}{q} + 1_A * 1_B(z) \right) ,
\end{aligned}$$

where we also observed that $1 * 1_A(z) = \mathbb{E}_{x \in \mathbb{F}_q}[1 \cdot 1_A(z - x)] = \frac{\ell}{q}$, and similarly $1 * 1_B(z) = \frac{\ell}{q}$. Thus, [Equation \(10\)](#) becomes

$$\begin{aligned}
& \sum_{z \in T} \left[(1 - \omega_1)(1 - \omega_2) \cdot \frac{q}{\ell^2} \cdot 1_A * 1_B(z) + (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \cdot \frac{q}{\ell(q - \ell)} \cdot \left(\frac{\ell}{q} - 1_A * 1_B(z) \right) \right. \\
& \quad \left. + \omega_1\omega_2 \cdot \frac{q}{(q - \ell)^2} \cdot \left(1 - 2 \cdot \frac{\ell}{q} + 1_A * 1_B(z) \right) \right] \\
&= \sum_{z \in T} \left((1 - \omega_1)(1 - \omega_2) \cdot \frac{q}{\ell^2} - (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \frac{q}{\ell(q - \ell)} + \rho^2 \cdot \frac{q}{(q - \ell)^2} \right) \cdot 1_A * 1_B(z) \\
& \quad + \ell \cdot \left[(\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \frac{q}{\ell(q - \ell)} \cdot \frac{\ell}{q} + \omega_1\omega_2 \frac{q}{(q - \ell)^2} \left(1 - 2 \cdot \frac{\ell}{q} \right) \right] \\
&= \left((1 - \omega_1)(1 - \omega_2) \cdot \frac{q}{\ell^2} - (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \frac{q}{\ell(q - \ell)} \right. \\
& \quad \left. + \omega_1\omega_2 \cdot \frac{q}{(q - \ell)^2} \right) \sum_{z \in T} 1_A * 1_B(z)
\end{aligned} \tag{11}$$

$$+ \frac{(\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1))\ell}{q - \ell} + \omega_1\omega_2 \cdot \frac{q\ell - 2\ell^2}{(q - \ell)^2} . \tag{12}$$

We first consider the term [Equation \(11\)](#). Let

$$c = (1 - \omega_1)(1 - \omega_2) \cdot \frac{q^2}{\ell^2} - (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \frac{q^2}{\ell(q - \ell)} + \omega_1\omega_2 \cdot \frac{q^2}{(q - \ell)^2} .$$

We claim that $c \geq 0$. Indeed, put $\alpha := \frac{\ell}{q}$, so $1 - \alpha = 1 - \frac{\ell}{q} = \frac{q - \ell}{q}$ and note that

$$c = \frac{(1 - \omega_1)(1 - \omega_2)}{\alpha^2} - \frac{\omega_1(1 - \omega_2)}{\alpha \cdot (1 - \alpha)} - \frac{\omega_2(1 - \omega_1)}{\alpha \cdot (1 - \alpha)} + \frac{\omega_1\omega_2}{1 - \alpha^2} .$$

Put $s = \frac{1 - \omega_1}{\alpha}$, $t = \frac{1 - \omega_2}{\alpha}$, $u = \frac{\omega_1}{1 - \alpha}$ and $v = \frac{\omega_2}{1 - \alpha}$, so then

$$c = st - sv - tu + uv = s(t - v) - u(t - v). \tag{13}$$

Since $\omega_1 < 1 - \alpha$, it follows that $u \leq 1 \leq s$, and similarly as $\omega_2 < 1 - \alpha$ we have $v \leq 1 \leq t$. Thus, looking at [Equation \(13\)](#), since $t - v \geq 0$ and $s \geq u$, it follows that $c \geq 0$, as claimed.

Thus, using the trivial upper bound $1_A * 1_B(z) \leq \frac{\ell}{q}$ valid for all $z \in \mathbb{F}_q$, we find

$$(11) = \frac{c}{q} \sum_{z \in T} 1_A * 1_B(z) \leq \frac{c}{q} \cdot \ell \cdot \frac{\ell}{q} = \frac{\ell^2}{q^2} \cdot c = \alpha^2 c.$$

We can expand

$$\begin{aligned} \alpha^2 \cdot c &= \alpha^2 \cdot \left(\frac{(1 - \omega_1)(1 - \omega_2)}{\alpha^2} - \frac{\omega_1(1 - \omega_2)}{\alpha \cdot (1 - \alpha)} - \frac{\omega_2(1 - \omega_1)}{\alpha \cdot (1 - \alpha)} + \frac{\omega_1 \omega_2}{1 - \alpha^2} \right) \\ &= (1 - \omega_1)(1 - \omega_2) - (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \cdot \frac{\alpha}{1 - \alpha} + \omega_1 \omega_2 \left(\frac{\alpha^2}{(1 - \alpha)^2} \right) \\ &= (1 - \omega_1)(1 - \omega_2) - (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \frac{\ell}{q - \ell} + \omega_1 \omega_2 \frac{\ell^2}{(q - \ell)^2}. \end{aligned}$$

Combining this again with [Equation \(12\)](#), we obtain the following upper bound:

$$\begin{aligned} &(1 - \omega_1)(1 - \omega_2) - (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \frac{\ell}{q - \ell} + \omega_1 \omega_2 \frac{\ell^2}{(q - \ell)^2} \\ &\quad + (\omega_1(1 - \omega_2) + \omega_2(1 - \omega_1)) \frac{\ell}{q - \ell} + \omega_1 \omega_2 \frac{q\ell - 2\ell^2}{(q - \ell)^2} \\ &= (1 - \omega_1)(1 - \omega_2) + \omega_1 \omega_2 \left(\frac{q\ell}{(q - \ell)^2} - \frac{\ell^2}{q - \ell} \right) \\ &= (1 - \omega_1)(1 - \omega_2) + \omega_1 \omega_2 \cdot \frac{\ell}{q - \ell} \left(\frac{q}{q - \ell} - \frac{\ell}{q - \ell} \right) \\ &= (1 - \omega_1)(1 - \omega_2) + \omega_1 \omega_2 \cdot \frac{\ell}{q - \ell} \left(\frac{q - \ell}{q - \ell} \right) = (1 - \omega_1)(1 - \omega_2) + \omega_1 \omega_2 \cdot \frac{\ell}{q - \ell}, \end{aligned}$$

as was to be shown. \square

In the sequel, we will need upper and lower bounds on the RHS of [Lemma 4.2](#) to $1 - \rho$. The following lemma establishes the required bounds.

Lemma 4.3. *Suppose q is a prime power, $1 \leq \ell \leq q$ is an integer and $\rho \in (0, 1 - \ell/q)$. Suppose $0 \leq \eta \leq \rho$ and $\rho - \eta \leq \omega_1, \omega_2 \leq \rho$. Then, the following inequalities hold:*

$$1 - \rho > (1 - \rho)^2 + \rho^2 \cdot \frac{\ell}{q - \ell}, \quad (14)$$

$$(1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell} > (1 - \omega_1)(1 - \omega_2) + \omega_1 \omega_2 \cdot \frac{\ell}{q - \ell}. \quad (15)$$

Proof. For [Equation \(14\)](#), observe that the quadratic

$$(1 - \rho) = (1 - \rho)^2 + \rho^2 \cdot \frac{\ell}{q - \ell},$$

has solutions $\rho = 0$ and $\rho = 1 - \ell/q$, from which it follows that

$$1 - \rho > (1 - \rho)^2 + \rho^2 \cdot \frac{\ell}{q - \ell} \quad \forall 0 < \rho < 1 - \frac{\ell}{q}, \quad (16)$$

as claimed.

We now consider [Equation \(15\)](#). Consider the function $g(\omega_1, \omega_2) = (1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell}$, defined for $(\omega_1, \omega_2) \in [\rho - \eta, \rho]^2$. To show [Equation \(15\)](#), it suffices to show that g is strictly maximized at the point $(\rho - \eta, \rho - \eta)$. If $\omega_1 > \rho - \eta$, we first argue $g(\rho - \eta, \omega_2) > g(\omega_1, \omega_2)$. Put $\varepsilon_1 = \omega_1 - (\rho - \eta) > 0$ and observe that

$$\begin{aligned} & g(\rho - \eta, \omega_2) - g(\omega_1, \omega_2) \\ &= \left((1 - (\omega_1 - \varepsilon_1))(1 - \omega_2) + (\omega_1 - \varepsilon_1)\omega_2 \cdot \frac{\ell}{q - \ell} \right) - \left((1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell} \right) \\ &= \varepsilon_1(1 - \omega_2) - \varepsilon_1\omega_2 \frac{\ell}{q - \ell} = \varepsilon_1 \left(1 - \omega_2 \left(1 + \frac{\ell}{q - \ell} \right) \right). \end{aligned}$$

Since $\omega_2 < 1 - \frac{\ell}{q}$, we observe that

$$\begin{aligned} \omega_2 \cdot \left(1 + \frac{\ell}{q - \ell} \right) &< \left(1 - \frac{\ell}{q} \right) \left(1 + \frac{\ell}{q - \ell} \right) = 1 - \frac{\ell}{q} + \frac{\ell}{q - \ell} - \frac{\ell^2}{q(q - \ell)} \\ &= 1 - \frac{\ell(q - \ell) - \ell q + \ell^2}{q(q - \ell)} = 1 - \frac{\ell q - \ell^2 - \ell q + \ell^2}{q(q - \ell)} = 1. \end{aligned}$$

Thus,

$$1 - \omega_2 \left(1 + \frac{\ell}{q - \ell} \right) > 0,$$

so $g(\rho - \eta, \omega_2) > g(\omega_1, \omega_2)$. By reversing the roles of ω_2 and ω_1 we find $g(\rho - \eta, \rho - \eta) \geq g(\rho - \eta, \omega_2)$ as well, establishing [Equation \(15\)](#). \square

We can now state and prove a lemma bounding the probability that a nontrivial linear combination of two uniform samples from a list-recovery ball lands in a shift of the list-recovery ball. Then, in [Corollary 4.6](#), we show how to set parameters to turn this into a statement about the δ -mixing of a list-recovery ball.

Lemma 4.4. *Let $n \in \mathbb{N}$, q a prime power, $1 \leq \ell \leq q$ an integer, and let $\rho \in (0, 1 - \ell/q)$. Let $T_1, \dots, T_n \subseteq \mathbb{F}_q$ be subsets, each of size ℓ . Fix $\eta > 0$ small enough so that*

$$1 - \rho > (1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell}.$$

Let $\alpha, \beta \in \mathbb{F}_q \setminus \{0\}$ and $y \in \mathbb{F}_q^n$, and let $X, X' \sim B_\rho(T_1 \times \dots \times T_n)$. Then,

$$\begin{aligned} & \Pr[\alpha X + \beta X' \in y + B_\rho(T_1 \times \dots \times T_n)] \\ & \leq 2\sqrt{2n} \cdot \exp_q(n(h_{q,\ell}(\rho - \eta) - h_{q,\ell}(\rho))) \\ & \quad + 2n \cdot \exp_q\left(-nD_q\left(1 - \rho \|(1 - \rho + \eta)^2 + (\rho - \eta)^2 \frac{\ell}{q - \ell}\right)\right). \end{aligned} \tag{17}$$

Remark 4.5. Since [Lemma 4.3](#) implies

$$1 - \rho > (1 - \rho)^2 + \rho^2 \cdot \frac{\ell}{q - \ell} \iff 0 < \rho < 1 - \frac{\ell}{q},$$

it follows that one can indeed choose η small enough to ensure

$$1 - \rho > (1 - \rho - \eta)^2 + (\rho + \eta)^2 \cdot \frac{\ell}{q - \ell}.$$

Later in [Corollary 4.6](#) we will show how to choose $\eta > 0$ to bound the two terms in [Equation \(17\)](#) by $q^{-\delta n}$ for a concrete $\delta > 0$ (which depends on ρ, ℓ, q).

Proof. Denote $B = B_\rho(T_1 \times \cdots \times T_n)$, and fix any nonzero $\alpha_1, \alpha_2 \in \mathbb{F}_q$, and $y \in \mathbb{F}_q^n$. Fix some $\eta \in (0, \rho)$ soon to be determined. Let $Z_1 \sim \alpha_1 \cdot B$, and $Z_2 \sim \alpha_2 \cdot B$. The strategy is to “massage” the distribution of (Z_1, Z_2) so that it is easier to analyze the probability that $Z_1 + Z_2 \in B + y$, and then apply [Lemma 4.2](#).

For each $i \in [n]$ and $j = 1, 2$, let $W_{j,i} = 1_{\{Z_{j,i} \notin \alpha_i \cdot T_i\}}$, and let $W_j = (W_{j,1}, \dots, W_{j,n})$ for $j = 1, 2$. By the law of total probability,

$$\begin{aligned}
\Pr[Z_1 + Z_2 \in y + B] &= \sum_{1 \leq w_1, w_2 \leq \lfloor \rho n \rfloor} \Pr[Z_1 + Z_2 \in y + B | \text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2] \\
&\quad \cdot \Pr[\text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2] \\
&\leq \sum_{\lceil (\rho - \eta)n \rceil \leq w_1, w_2 \leq \lfloor \rho n \rfloor} \Pr[Z_1 + Z_2 \in y + B | \text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2] \\
&\quad \cdot \Pr[\text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2] \\
&\quad + \Pr[\text{wt}(W_1) \leq (\rho - \eta)n \vee \text{wt}(W_2) \leq (\rho - \eta)n] \\
&\leq \max_{\lceil (\rho - \eta)n \rceil \leq w_1, w_2 \leq \lfloor \rho n \rfloor} \Pr[Z_1 + Z_2 \in y + B | \text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2] \quad (18) \\
&\quad + \Pr[\text{wt}(W_1) \leq (\rho - \eta)n \vee \text{wt}(W_2) \leq (\rho - \eta)n].
\end{aligned}$$

We first bound

$$\begin{aligned}
\Pr[\text{wt}(W_1) \leq (\rho - \eta)n \vee \text{wt}(W_2) \leq (\rho - \eta)n] &\leq 2 \cdot \frac{|B_{\rho - \eta}(T_1 \times \cdots \times T_n)|}{|B_\rho(T_1 \times \cdots \times T_n)|} \\
&\leq 2 \cdot \frac{q^{h_{q,\ell}(\rho - \eta)n}}{\frac{1}{\sqrt{2n}} q^{nh_{q,\ell}(\rho)}} = 2\sqrt{2n} \cdot q^{(h_{q,\ell}(\rho - \eta) - h_{q,\ell}(\rho))n}, \quad (19)
\end{aligned}$$

where we used [Proposition 2.6](#).

We now focus on proving that [Equation \(18\)](#) is small. Fix any $w_1, w_2 \in \{\lceil (\rho - \eta)n \rceil, \lceil (\rho - \eta)n \rceil + 1, \dots, \lfloor \rho n \rfloor\}$ which maximize $\Pr[Z_1 + Z_2 \in y + B | \text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2]$, and set $\omega_j = w_j/n$ for $j = 1, 2$. We now introduce a “model” distribution for $Z_1 + Z_2 | (\text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2)$ which is easier to analyze. For $i = 1, \dots, n$ and $j = 1, 2$, let $A_{j,i} \in \{0, 1\}$ denote i.i.d. draws from a $\text{Ber}(\omega_j)$ random variable, and set $A_j = (A_{j,1}, \dots, A_{j,n})$.

Next, define for $i = 1, \dots, n$ the following random variables D_i :

$$D_i = \begin{cases} \alpha_1 \cdot X + \alpha_2 \cdot X' & A_{1,i} = A_{2,i} = 0, \\ \alpha_1 \cdot X + Y' & A_{1,i} = 0, A_{2,i} = 1, \\ Y + \alpha_2 \cdot X' & A_{1,i} = 1, A_{2,i} = 0, \\ Y + Y' & A_{1,i} = A_{2,i} = 1. \end{cases}$$

Above, $X, X' \sim T_i$, $Y \sim \mathbb{F}_q \setminus \alpha_1 T_i$, and $Y' \sim \mathbb{F}_q \setminus \alpha_2 T_i$, and they are all independent. Let $D = (D_1, \dots, D_n)$, and note that

$$\begin{aligned}
\Pr[Z_1 + Z_2 \in y + B | \text{wt}(Y_1) = w_1, \text{wt}(Y_2) = w_2] &= \Pr[D \in y + B | \text{wt}(A_1) = w_1, \text{wt}(A_2) = w_2] \\
&= \frac{\Pr[D \in y + B, \text{wt}(A_1) = w_1, \text{wt}(A_2) = w_2]}{\Pr[\text{wt}(A_1) = w_1, \text{wt}(A_2) = w_2]}
\end{aligned}$$

$$\begin{aligned}
&\leq \frac{\Pr[D \in y + B]}{\Pr[\text{wt}(A_1) = w_1, \text{wt}(A_2) = w_2]} \\
&\leq 2n \cdot \Pr[D \in y + B],
\end{aligned}$$

where the ultimate inequality follows from [Proposition 2.14](#).

We now focus on upper-bounding $\Pr[D \in y + B]$. Define the indicator random variables $E_i = 1_{\{D_i \in y_i + T_i\}}$ and note that $D \in y + B \iff \sum_{i=1}^n E_i \geq (1 - \rho)n$. Using the above notation, we find

$$\begin{aligned}
\Pr[E_i = 1] &= \Pr[D_i \in y + T_i] \\
&= \Pr[D_i \in y + T_i | A_{1,i} = A_{2,i} = 0] \Pr[A_{1,i} = A_{2,i} = 0] \\
&\quad + \Pr[D_i \in y + T_i | A_{1,i} = 0, A_{2,i} = 1] \Pr[A_{1,i} = 0, A_{2,i} = 1] \\
&\quad + \Pr[D_i \in y + T_i | A_{1,i} = 1, A_{2,i} = 0] \Pr[A_{1,i} = 1, A_{2,i} = 0] \\
&\quad + \Pr[D_i \in y + T_i | A_{1,i} = A_{2,i} = 1] \Pr[A_{1,i} = A_{2,i} = 1] \\
&= \Pr[\alpha_1 \cdot X + \alpha_2 \cdot X' \in y + T_i] \cdot (1 - \omega_1)(1 - \omega_2) \\
&\quad + \Pr[\alpha_1 \cdot X + Y' \in y + T_i | A_{1,i} = 0, A_{2,i} = 1] \cdot (1 - \omega_1)\omega_2 \\
&\quad + \Pr[Y + \alpha_2 \cdot X' \in y + T_i | A_{1,i} = 1, A_{2,i} = 0] \cdot \omega_1(1 - \omega_2) \\
&\quad + \Pr[Y + Y' \in y + T_i | A_{1,i} = A_{2,i} = 1] \cdot \omega_1\omega_2.
\end{aligned}$$

Applying [Lemma 4.2](#) with $A \leftarrow \alpha_1 T_i$ and $B \leftarrow \alpha_2 T_i$, noticing that $\omega_1, \omega_2 < 1 - \ell/q$, we readily get

$$\Pr[E_i = 1] \leq (1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell}.$$

Thus, if $F \sim \text{Binomial}(n, (1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell})$, then the probability that $\sum_{i=1}^n E_i \geq (1 - \rho)n$ is at most the probability that $F \geq (1 - \rho)n$. By the classical Chernoff–Hoeffding bound ([Proposition 2.10](#)),

$$\Pr[F \geq (1 - \rho)n] \leq \exp_q \left(-n D_q \left(1 - \rho \left\| (1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell} \right\| \right) \right).$$

Recall that $\rho - \eta \leq \omega_1, \omega_2 \leq \rho$, so by [Lemma 4.3](#),

$$(1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell} \leq (1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell}.$$

Thus, using [Claim 2.12](#), it follows that

$$D_q \left(1 - \rho \left\| (1 - \omega_1)(1 - \omega_2) + \omega_1\omega_2 \cdot \frac{\ell}{q - \ell} \right\| \right) \geq D_q \left(1 - \rho \left\| (1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell} \right\| \right).$$

It thus follows that

$$\begin{aligned}
&\max_{\lceil (\rho - \eta)n \rceil \leq w_1, w_2 \leq \lfloor \rho n \rfloor} \Pr[Z_1 + Z_2 \in y + B | \text{wt}(W_1) = w_1, \text{wt}(W_2) = w_2] \\
&\leq 2n \cdot \Pr[D \in y + B] \\
&\leq 2n \cdot \exp_q \left(D_q \left(1 - \rho \left\| (1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell} \right\| \right) \right),
\end{aligned}$$

which, when combined with the bound of [Equation \(19\)](#), yields the bound claimed in the lemma. \square

Corollary 4.6. *Let $n \in \mathbb{N}$, q a prime power, $1 \leq \ell < q$ an integer, and let $\rho \in (0, 1 - \ell/q)$. Let $T_1, \dots, T_n \subseteq \mathbb{F}_q$, each of size ℓ . The list-recovery ball $B_\rho(T_1 \times \dots \times T_n)$ is δ -mixing, for*

$$\delta = \log_q \left(\frac{(q - \ell)(1 - \rho)}{\rho \ell} \right) \cdot \frac{\rho^4(1 - \ell/q - \rho)^2}{16 \log q}$$

assuming $n \geq \left(\frac{\log q}{\rho(1 - \ell/q - \rho)} \right)^c$ for some universal constant c .

Proof. By [Lemma 4.4](#), it suffices to show that we can choose $\eta > 0$ so that

$$1 - \rho > (1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell}$$

and, that assuming $n \geq \left(\frac{\log q}{\rho(1 - \ell/q - \rho)} \right)^c$ for universal constant c , we have

$$(2\sqrt{2n}) \cdot \exp_q(n(h_{q,\ell}(\rho - \eta) - h_{q,\ell}(\rho))) \tag{20}$$

$$+ 2n \exp_q \left(-n D_q \left(1 - \rho \|(1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell} \right) \right) \tag{21}$$

$$\leq q^{-n\delta},$$

for δ as in the statement.

Set $\gamma = \frac{\ell}{q - \ell}$. Note that then $0 < \rho < 1 - \ell/q$ is equivalent to $0 < \rho < \frac{1}{1 + \gamma}$. Define Δ so that

$$1 - \rho - \Delta = (1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \gamma,$$

which means that

$$\begin{aligned} \Delta &= (1 + 2\eta + 2\eta\gamma)\rho - (1 + \gamma)\rho^2 - 2\eta - \eta^2 - \eta^2\gamma \\ &\geq (1 + 2\eta + 2\eta\gamma)\rho - (1 + \gamma)\rho^2 - (3 + \gamma)\eta. \end{aligned} \tag{22}$$

Rearranging, we get that [Equation \(22\)](#) is at least $\eta\rho$ whenever

$$0 < \eta \leq \frac{\rho - \rho^2(1 + \gamma)}{(3 + \gamma) - \rho(1 + 2\gamma)}.$$

Given this, we may choose

$$\eta = \frac{\rho(1 - \ell/q - \rho)}{3} > 0.$$

Indeed, recalling that $\gamma = \frac{\ell}{q - \ell}$, we have

$$\frac{\rho - \rho^2(1 + \gamma)}{(3 + \gamma) - \rho(1 + 2\gamma)} \geq \frac{\rho - \rho^2(1 + \gamma)}{3 + \gamma} = \frac{\rho(q(1 - \rho) - \ell)}{3q - 2\ell} \geq \frac{\rho(q(1 - \rho) - \ell)}{3q} = \eta.$$

By [Claim 2.13](#), $D(1 - \rho\|1 - \rho - \Delta) \leq 2\Delta^2$, and so $D_q(1 - \rho\|1 - \rho - \Delta) \leq \frac{2}{\ln q}\Delta^2$. We therefore have

$$\begin{aligned} 2n \exp_q \left(-n D_q \left(1 - \rho \|(1 - \rho + \eta)^2 + (\rho - \eta)^2 \cdot \frac{\ell}{q - \ell} \right) \right) &\leq 2n \exp_q \left(-\frac{2}{\ln q} \eta^2 \rho^2 n \right) \\ &\leq \exp_q \left(-\frac{\rho^4(1 - \ell/q - \rho)^2}{16 \log q} \cdot n \right), \end{aligned} \tag{23}$$

assuming that $n \geq \text{poly}(\log q, 1/\rho, 1/(1 - \ell/q - \rho))$.

We now obtain a lower bound on $h_{q,\ell}(\rho) - h_{q,\ell}(\rho - \eta)$ with our chosen η . [Claim 2.9](#) tells us that

$$h_{q,\ell}(\rho) - h_{q,\ell}(\rho - \eta) \geq \log_q \left(\frac{(q - \ell)(1 - \rho)}{\rho \ell} \right) \eta = \log_q \left(\frac{(q - \ell)(1 - \rho)}{\rho \ell} \right) \cdot \frac{\rho(1 - \ell/q - \rho)}{3},$$

which is positive whenever $\rho < 1 - \ell/q$. Thus,

$$\begin{aligned} 2\sqrt{2n} \cdot \exp_q \left(-\log_q \left(\frac{(q - \ell)(1 - \rho)}{\rho \ell} \right) \frac{\rho(1 - \ell/q - \rho)}{3} \cdot n \right) \\ \leq \exp_q \left(-\log_q \left(\frac{(q - \ell)(1 - \rho)}{\rho \ell} \right) \frac{\rho(1 - \ell/q - \rho)}{6} \cdot n \right), \end{aligned} \quad (24)$$

where we assumed that $n \geq \text{poly}(\log q, 1/\rho, 1/(1 - \ell/q - \rho))$.

By [Equations \(23\)](#) and [\(24\)](#), it follows that a rough, but sufficient, bound on [\(20\)](#)+[\(21\)](#) is

$$\exp_q \left(-\log_q \left(\frac{(q - \ell)(1 - \rho)}{\rho \ell} \right) \cdot \frac{\rho^4(1 - \ell/q - \rho)^2}{16 \log q} \cdot n \right),$$

completing the proof. \square

4.2 List Recovery from Errors

Having established that the list-recovery ball is δ -mixing, we can repeat roughly the same argument we had for list recovery with erasures, using [Lemma 3.4](#).

Theorem 4.7 (list recovery with errors). *For every $n \in \mathbb{N}$, a prime power q , an integer $\ell < q$, $\rho \in (0, 1 - \ell/q)$, and $\varepsilon \in (0, 1)$, the following holds. With probability at least $1 - q^{-n}$, a random linear code $\mathcal{C} \subseteq \mathbb{F}_q^n$ of rate*

$$R = 1 - h_{q,\ell}(\rho) - \varepsilon$$

is (ρ, ℓ, L) -list-recoverable from errors, with

$$L = C_{\rho,\ell,q} \cdot \frac{1}{\varepsilon},$$

provided that n is large enough. More concretely, there exists a universal constant C such that

$$C_{\rho,\ell,q} \leq q^{\ell \cdot \left(\frac{\log q}{\rho(1 - \ell/q - \rho)} \right)^C}$$

provided that $n \geq \left(\frac{\log q}{\rho(1 - \ell/q - \rho)} \right)^C$.

Proof. The technique follows the proof of [Theorem 3.5](#), with the necessary changes. We fix some $T_1, \dots, T_n \subseteq \mathbb{F}_q$, each of size ℓ , and denote by $T = B_\rho(T_1 \times \dots \times T_n)$ the list-recovery ball. Recall that we wish to show that $|T \cap \mathcal{C}| \leq L$. The rest of the argument exactly matches [Theorem 3.5](#), that is, if $|T \cap \mathcal{C}| > L$, there must exist some $\mathbf{v} \in \mathcal{F}$ for which $\{\mathbf{v}\} \subseteq T \cap \mathcal{C}$. Three things change:

1. Our bound on δ , which we now take from [Corollary 4.6](#).
2. The number of input lists we union-bound over. While in [Theorem 3.5](#) it was $\mathcal{T} = \binom{n}{\alpha n} \binom{q}{\ell}^{(1-\alpha)n}$, here it's $\mathcal{T} = \binom{q}{\ell}^n$.

3. The gap ε is now with respect to the “list-recovery with *errors*” capacity $1 - h_{q,\ell}(\rho)$.

Concretely, the bound on p_1 now becomes

$$p_1 \leq \mathcal{T} \cdot b^\star q^{-an} \cdot \sum_{b=\log_q(L+1)}^{b^\star} |T|^b \cdot q^{-(1-R)nb},$$

and the bound on p_2 is now

$$p_2 \leq \mathcal{T} \cdot \sum_{b=b^\star+1}^{L+1} |T|^b q^{-(1-R)nb},$$

and we are interested in bounding $p = p_1 + p_2$. We will re-set a and c (which appears in $b^\star = \lceil c\ell/\varepsilon \rceil$) shortly. Recalling that $|T| \leq q^{nh_{q,\ell}(\rho)}$ (see [Proposition 2.6](#)), the bound on p_1 becomes

$$\begin{aligned} p_1 &\leq q^{n\ell \log_q(eq/\ell) + \log_q(b^\star) - an} \cdot \sum_{b=\log_q(L+1)}^{b^\star} q^{nbh_{q,\ell}(\rho) - (h_{q,\ell}(\rho) + \varepsilon)nb} \\ &\leq q^{2n\ell - an - \varepsilon n h_{q,\ell}(\rho) \log_q(L+1)} \leq q^{(2\ell - a)n}. \end{aligned}$$

Taking $a = 2\ell + 2$, we get $p_1 \leq q^{-2n}$. Moving on to p_2 , we have

$$p_2 \leq \mathcal{T} \cdot \sum_{b=b^\star+1}^{L+1} q^{nbh_{q,\ell}(\rho) - (h_{q,\ell}(\rho) + \varepsilon)nb} \leq q^{2n\ell - h_{q,\ell}(\rho)\varepsilon nb^\star}.$$

Setting $c = \frac{1}{4h_{q,\ell}(\rho)}$ we get $p_2 \leq q^{-2n}$, and overall $p \leq q^{-n}$, as desired. The output list size is $q^{\frac{8a}{\delta} \cdot \frac{c\ell}{\varepsilon}}$. Using the fact that $\frac{1}{h_{q,\ell}(\rho)} \leq \frac{1}{\log q}$, and that $\log_q\left(\frac{(q-\ell)(1-\rho)}{\rho\ell}\right) \leq \log_q(q/\rho)$, the bound on $C_{q,\rho}$ follows. \square

Acknowledgements

This work was done in part while the authors were visiting the Simons Institute for the Theory of Computing, supported by DOE grant #DE-SC0024124. D. Doron is supported in part by NSF-BSF grant #2022644. J. Mosheiff is supported by Israel Science Foundation grant 3450/24 and an Alon Fellowship. N. Resch is supported by an NWO (Dutch Research Council) grant with number C.2324.0590. J. Ribeiro is supported by FCT/MECI through national funds and when applicable co-funded EU funds under UID/50008: Instituto de Telecomunicações.

References

- [BDT20] Avraham Ben-Aroya, Dean Doron, and Amnon Ta-Shma. Near-optimal erasure list-decodable codes. In *35th Computational Complexity Conference (CCC)*, pages 1:1–1:27. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020.
- [CT06] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. John Wiley & Sons, 2nd edition, 2006.
- [CZ24] Yeyuan Chen and Zihan Zhang. Explicit folded Reed-Solomon and multiplicity codes achieve relaxed generalized Singleton bounds, 2024. <https://arxiv.org/abs/2408.15925>.

- [DMOZ22] Dean Doron, Dana Moshkovitz, Justin Oh, and David Zuckerman. Nearly optimal pseudorandomness from hardness. *Journal of the ACM*, 69(6), November 2022.
- [DW22] Dean Doron and Mary Wootters. High-probability list-recovery, and applications to heavy hitters. In *49th International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 55:1–55:17. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.
- [Eli57] Peter Elias. List decoding for noisy channels, 1957. <https://dspace.mit.edu/handle/1721.1/4484>.
- [GHK11] Venkatesan Guruswami, Johan Håstad, and Swastik Kopparty. On the list-decodability of random linear codes. *IEEE Transactions on Information Theory*, 57(2):718–725, 2011. Preliminary version at STOC 2010.
- [GI02] Venkatesan Guruswami and Piotr Indyk. Near-optimal linear-time codes for unique decoding and new list-decodable codes over smaller alphabets. In *34th Annual Symposium on Theory of Computing (STOC)*, pages 812–821. ACM, 2002.
- [GI03] Venkatesan Guruswami and Piotr Indyk. Linear time encodable and list decodable codes. In *35th Annual Symposium on Theory of Computing (STOC)*, pages 126–135. ACM, 2003.
- [GI04] Venkatesan Guruswami and Piotr Indyk. Efficiently decodable codes meeting Gilbert-Varshamov bound for low rates. In *15th Annual Symposium on Discrete Algorithms (SODA)*, pages 756–757. SIAM, 2004.
- [GI05] Venkatesan Guruswami and Piotr Indyk. Linear-time encodable/decodable codes with near-optimal rate. *IEEE Transactions on Information Theory*, 51(10):3393–3400, 2005.
- [GKO⁺18] Sivakanth Gopi, Swastik Kopparty, Rafael Oliveira, Noga Ron-Zewi, and Shubhangi Saraf. Locally testable and locally correctable codes approaching the Gilbert-Varshamov bound. *IEEE Transactions on Information Theory*, 64(8):5813–5831, 2018.
- [GLM⁺22] Venkatesan Guruswami, Ray Li, Jonathan Mosheiff, Nicolas Resch, Shashwat Silas, and Mary Wootters. Bounds for list-decoding and list-recovery of random linear codes. *IEEE Transactions on Information Theory*, 68(2):923–939, 2022.
- [GLPS17] Anna C. Gilbert, Yi Li, Ely Porat, and Martin J. Strauss. For-all sparse recovery in near-optimal time. *ACM Transactions on Algorithms*, 13(3):1–26, 2017.
- [GLS⁺21] Zeyu Guo, Ray Li, Chong Shangguan, Itzhak Tamo, and Mary Wootters. Improved list-decodability and list-recoverability of Reed-Solomon codes via tree packings. In *62nd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 708–719. IEEE, 2021.
- [GR18] Venkatesan Guruswami and Nicolas Resch. On the list-decodability of random linear rank-metric codes. In *International Symposium on Information Theory (ISIT)*, pages 1505–1509. IEEE, 2018.
- [GST22] Eitan Goldberg, Chong Shangguan, and Itzhak Tamo. Singleton-type bounds for list-decoding and list-recovery, and related results. In *International Symposium on Information Theory (ISIT)*, pages 2565–2570. IEEE, 2022.

- [Gur03] Venkatesan Guruswami. List decoding from erasures: Bounds and code constructions. *IEEE Transactions on Information Theory*, 49(11):2826–2833, 2003.
- [GUV09] Venkatesan Guruswami, Christopher Umans, and Salil P. Vadhan. Unbalanced expanders and randomness extractors from Parvaresh-Vardy codes. *Journal of the ACM*, 56(4):20:1–20:34, 2009.
- [HIOS15] Iftach Haitner, Yuval Ishai, Eran Omri, and Ronen Shaltiel. Parallel hashing via list recoverability. In *Advances in Cryptology – CRYPTO 2015*, pages 173–190. Springer Berlin Heidelberg, 2015.
- [HLR21] Justin Holmgren, Alex Lombardi, and Ron D. Rothblum. Fiat–Shamir via list-recoverable codes (or: parallel repetition of GMW is not zero-knowledge). In *53rd Annual Symposium on Theory of Computing (STOC)*, pages 750–760. ACM, 2021.
- [HRW20] Brett Hemenway, Noga Ron-Zewi, and Mary Wootters. Local list recovery of high-rate tensor codes and applications. *SIAM Journal on Computing*, 49(4):FOCS17–157, January 2020.
- [INR10] Piotr Indyk, Hung Q. Ngo, and Atri Rudra. Efficiently decodable non-adaptive group testing. In *21st Annual Symposium on Discrete Algorithms (SODA)*, pages 1126–1142. SIAM, 2010.
- [KM25] Sergey Komech and Jonathan Mosheiff. Let’s have both! Optimal list-recoverability via alphabet permutation codes, 2025. <https://www.arxiv.org/abs/2502.05858>.
- [KMRS17] Swastik Kopparty, Or Meir, Noga Ron-Zewi, and Shubhangi Saraf. High-rate locally correctable and locally testable codes with sub-polynomial query complexity. *Journal of the ACM*, 64(2):1–42, 2017.
- [KRSW18] Swastik Kopparty, Noga Ron-Zewi, Shubhangi Saraf, and Mary Wootters. Improved decoding of folded Reed-Solomon and multiplicity codes. In *59th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 212–223. IEEE, 2018.
- [KT22] Itay Kalev and Amnon Ta-Shma. Unbalanced expanders from multiplicity codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM)*, pages 12:1–12:14. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2022.
- [Lev01] Vsevolod F. Lev. Linear equations over \mathbb{F}_p and moments of exponential sums. *Duke Mathematical Journal*, 107(2):239–263, 2001.
- [LMS24] Matan Levi, Jonathan Mosheiff, and Nikhil Shagrithaya. Random Reed-Solomon codes and random linear codes are locally equivalent, 2024. <https://arxiv.org/abs/2406.02238>.
- [LNNT16] Kasper Green Larsen, Jelani Nelson, Huy L. Nguyen, and Mikkel Thorup. Heavy hitters via cluster-preserving clustering. In *57th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 61–70. IEEE, 2016.
- [LP20] Ben Lund and Aditya Potukuchi. On the list recoverability of randomly punctured codes. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms*

- and Techniques (APPROX/RANDOM), pages 30:1–30:11. Schloss Dagstuhl – Leibniz-Zentrum für Informatik, 2020.
- [LS25] Ray Li and Nikhil Shagrithaya. Near-optimal list-recovery of linear code families, 2025. <https://arxiv.org/abs/2502.13877>.
 - [MRSY24] Jonathan Mosheiff, Nicolas Resch, Kuo Shang, and Chen Yuan. Randomness-efficient constructions of capacity-achieving list-decodable codes, 2024. <https://arxiv.org/abs/2402.11533>.
 - [NPR11] Hung Q. Ngo, Ely Porat, and Atri Rudra. Efficiently decodable error-correcting list disjoint matrices and applications. In *International Colloquium on Automata, Languages, and Programming (ICALP)*, pages 557–568. Springer, 2011.
 - [Res20] Nicolas Resch. *List-Decodable Codes: (Randomized) Constructions and Applications*. PhD thesis, Carnegie Mellon University, 2020. <http://reports-archive.adm.cs.cmu.edu/anon/2020/abstracts/20-113.html>.
 - [RW14] Atri Rudra and Mary Wootters. Every list-decodable code for high noise has abundant near-optimal rate puncturings. In *46th Annual Symposium on Theory of Computing (STOC)*, pages 764–773. ACM, 2014.
 - [RW18] Atri Rudra and Mary Wootters. Average-radius list-recoverability of random linear codes. In *29th Annual Symposium on Discrete Algorithms (SODA)*, pages 644–662. SIAM, 2018.
 - [Tam24] Itzhak Tamo. Tighter list-size bounds for list-decoding and recovery of folded Reed-Solomon and multiplicity codes. *IEEE Transactions on Information Theory*, 70(12):8659–8668, 2024.
 - [TZ04] Amnon Ta-Shma and David Zuckerman. Extractor codes. *IEEE Transactions on Information Theory*, 50(12):3015–3025, 2004.
 - [WR61] John Wozencraft and Barney Reiffen. *Sequential Decoding*. MIT Press, 1961.
 - [ZP81] Victor Vasilievich Zyablov and Mark Semenovich Pinsker. List concatenated decoding. *Problemy Peredachi Informatsii*, 17(4):29–33, 1981.