Repairable Fountain Codes

Megasthenis Asteris, *Student Member, IEEE,* Alexandros G. Dimakis, *Member, IEEE*

Abstract—We introduce a new family of Fountain codes that are systematic and also have sparse parities. Given an input of k symbols, our codes produce an unbounded number of output symbols, generating each parity independently by linearly combining a logarithmic number of randomly selected input symbols. The construction guarantees that for any $\epsilon > 0$ accessing a random subset of $(1 + \epsilon)k$ encoded symbols, asymptotically suffices to recover the k input symbols with high probability.

Our codes have the additional benefit of logarithmic locality: a single lost symbol can be repaired by accessing a subset of $O(\log k)$ of the remaining encoded symbols. This is a desired property for distributed storage systems where symbols are spread over a network of storage nodes. Beyond recovery upon loss, local reconstruction provides an efficient alternative for reading symbols that cannot be accessed directly. In our code, a logarithmic number of disjoint local groups is associated with each systematic symbol, allowing *multiple parallel reads*.

Our main mathematical contribution involves analyzing the rank of sparse random matrices with specific structure over finite fields. We rely on establishing that a new family of sparse random bipartite graphs have perfect matchings with high probability.

Index Terms—Systematic Fountain code, Logarithmic locality, Availability.

I. INTRODUCTION

FOUNTAIN codes [2], [3], [4] form a new family of linear erasure codes with several attractive properties. For a given set of k input symbols, a Fountain code produces a potentially limitless stream of output symbols, each created independently of others as a random combination of input symbols according to a given distribution. Ideally, given a randomly selected subset of $(1+\epsilon)k$ encoded symbols, a decoder should be able to recover the original k input symbols with high probability (w.h.p.) for some small overhead ϵ. Further, Fountain codes typically emphasize on efficient encoding and decoding algorithms.

In this work, we design a new family of Fountain codes that combine multiple properties appealing to distributed storage. One property that is highly desired for distributed storage codes is *systematic form*: the original information symbols must appear in the encoded sequence. Their presence enables the reading of source data without decoding and is a practical requirement for most storage applications. Another important property of distributed storage codes is efficient *repair* [5], [6], [7]: when a single encoded symbol is lost it should be possible to reconstruct it without communicating too much

information from other encoded symbols. A related property is that of *locality* of each symbol: the number of encoded symbols that need to be accessed to reconstruct that particular symbol [8], [9], [10], [11].

A key observation is that in a systematic linear code, locality is strongly connected to the sparsity of parity symbols [11], *i.e.*, the maximum number of input symbols combined in a parity symbol. A parity symbol along with the systematic symbols covered by it form a *local group*. Any symbol in this group can be reconstructed via an appropriate linear combination of the remaining member symbols. The smaller the size of the local group, the lower the locality of the symbols in it.

In existing Fountain codes, such as LT or Raptor codes, each encoded symbol is a linear combination of $O(\log k)$ or even constant number of input symbols on average. However, these codes are not systematic and the low degree of the encoded symbols does not imply low locality. Certain classes, such as Raptor codes, can be transformed into a systematic form [4] via a preprocessing of the input. Unfortunately, due to the additional step, parity symbols are no longer sparse in the original input symbols.

Standard Fountain codes support computationally efficient encoding and decoding algorithms as a result of a meticulously designed encoded symbol degree distribution. Fast decoding algorithms, however, do not translate to efficient repair: these algorithms aim at retrieving the entire source message from a set of available symbols, and are not tailored to the needs of a single symbol reconstruction. On the contrary, single erasures – the most frequent scenario in a distributed storage setting – can be efficiently repaired by an erasure code featuring low locality. If additionally the code is in systematic form, full scale decoding is invoked only in the unlikely event of multiple erasures that cannot be locally repaired. In other words, the presence of the source data in the encoded sequence in conjunction with low locality renders decoding an infrequently used operation, downgrading the need for efficient decoding algorithms.

The significance of locality is not limited to the repair problem, *i.e.*, the reconstruction of a symbol upon its loss. It extends to the closely related use case of *degraded reads*. In a distributed setup each symbol is stored on a different storage node, which may be temporarily unavailable due to a variety of reasons. Although not permanently lost, a systematic symbol may not be directly accessible, and its local group provides an efficient alternative for reading it. The *availability* of a systematic symbol naturally extends the notion of locality, measuring the number of disjoint local groups the symbol belongs to. We define the *availability* of a systematic symbol as the number of disjoint sets of encoded symbols which

can be used to reconstruct that particular symbol. In effect, it characterizes the number of read requests for a particular systematic symbol that can be simultaneously served.

Our Contribution: We introduce a new family of Fountain codes that are systematic and also have parity symbols with logarithmic sparsity. We show that this is impossible if we require the code to be MDS, but is possible if we require a near-MDS property similar to the probabilistic guarantees provided by LT and Raptor codes.

More concretely, for any $\epsilon > 0$ we construct codes that guarantee that a random subset of $(1+\epsilon)k$ symbols suffices to recover the original k input symbols w.h.p. Our codes produce an unbounded number of output symbols, creating each parity independently by linearly combining a logarithmic number of randomly chosen input symbols.

We show that this structure also provides logarithmic locality: each symbol in our codes is repairable by accessing only $O(\log k)$ other coded symbols. We further define the notion of symbol availability and show that the systematic symbols in our codes feature logarithmic availability: with high probability, for each systematic symbol there exist $O(\log k)$ disjoint sets of symbols that can be used to reconstruct it. This means that multiple parallel jobs can read this symbol concurrently, each by accessing one disjoint set. This new property is motivated by the straggler performance bottlenecks observed recently in distributed storage systems [12].

One disadvantage of our construction is higher decoding complexity. Our codes can be decoded by solving a system of linear equations over $\mathbb{F}_q$, which corresponds to maximum likelihood decoding for the erasure channel. This naive decoding can be implemented using Gaussian elimination and requires $O(k^3)$ steps. Fortunately, the matrices we construct are sparse, allowing faster decoding: Wiedemann's algorithm [13] can be used to decode in $O(k^2 \text{polylog} k)$ time. Standard Fountain codes create linear equations that can be solved just by back-substitution which amounts to decoding complexities of $O(k \log k)$ for LT [3] and $O(k)$ for Raptor [4] but offer no locality. It remains open to construct Fountain codes that have locality and near-linear decoding complexity.

Our main technical contribution is a novel random matrix result: we show that a family of random matrices with non independent entries have full rank with high probability. The analysis builds on the connections of matrix determinants to flows on random bipartite graphs, using techniques from [14], [15]. Our key result is showing that a new family of sparse random graphs have matchings w.h.p. Our random graph contribution is explained in Section V.

II. PROBLEM DESCRIPTION

Given k input symbols, elements of a finite field $\mathbb{F}_q$, we want to encode them into n symbols using a linear code. Linear codes are described by a $k \times n$ *generator* matrix $\mathbf{G}$ over $\mathbb{F}_q$, which when multiplied by an input vector $\mathbf{u} \in \mathbb{F}_q^{1 \times k}$ produces a codeword $\mathbf{v} = \mathbf{uG} \in \mathbb{F}_q^{1 \times n}$. Ideally, we would like $\mathbf{G}$ to have the following properties:

- *Systematic form*, i.e., a subset of the columns of $\mathbf{G}$ forms the identity matrix, $\mathbf{I}$, which implies that the input symbols are reproduced in the encoded sequence.

- *Rateless property*, i.e., each column is created independently. The number n of columns does not have to be specified for the encoder a priori. Equivalently, encoded symbols can be created or removed dynamically upon request, without recreating the entire encoded sequence.
- *MDS property*, i.e., any k columns of $\mathbf{G}$ have rank k, implying that any subset of k encoded symbols suffices to retrieve the input.
- *Low locality*. $\mathbf{G}$ has *locality* l if each column can be written as a linear combination of at most l other columns. If the code is systematic, then sparse parities suffice to obtain good locality [11].
- *High Availability*. A systematic symbol has *availability* t if it can be written as a linear combination of t disjoint sets of symbols, of cardinality l. The code has availability t', equal to that of the least available systematic symbol.

For any code, any sufficiently large subset of encoded symbols should allow recovery of the original data. The size of such a set is tightly related to the reliability of the code. For optimal reliability, i.e., in the case of MDS codes, an information theoretically minimum subset of k encoded symbols suffices to decode. When equipped with systematic form, the generator matrix of an MDS code affords no zero coefficient in the parity generating columns. To verify that, consider a parity column with a zero coefficient in the i-th position: that parity column along with any $k-1$ systematic columns excluding the one corresponding to the i-th systematic symbol form a singular matrix.

If parities are deliberately sparse in the input symbols, seeking to improve the code's *locality*, the property that any k encoded symbols suffice to retrieve the original data has to be relaxed. In this work, we require that for $\epsilon > 0$, a set of $k' = (1 + \epsilon)k$ randomly selected encoded symbols suffice to decode with high probability; the decoder may fail, but with a probability vanishing polynomially in k. We refer to a code with this property as *near-MDS*.

Under this constraint, we seek codes that achieve optimal locality, which translates into determining how sparse the parities can be without violating the decoding guarantee. We will show that it is impossible to recover the original message with high probability if the parities are linear combinations of fewer than $\Omega(\log k)$ input symbols. Furthermore, we will design codes that achieve logarithmic sparsity in the parities and hence, order optimal locality. We conclude the paper investigating the availability of our construction, showing that with high probability every systematic symbol belongs to a logarithmic number of disjoint local groups.

III. PRIOR WORK

In LT codes, the first practical realizations of Fountain codes invented by Luby [3], the average degree of the output symbols, i.e., the number of input symbols combined into an output symbol, is $O(\log k)$. Note, however, that sparsity in this case does not imply good locality, since LT codes lack systematic form.

Building on LT, Shokrollahi in [4] introduced Raptor codes, a different class of Fountain codes. The core idea is to precode the input symbols prior to the application of an appropriate

LT code. By virtue of the two layer encoding, the per symbol encoding cost – which corresponds to average degree of encoded symbols – is reduced to a constant, while the k input symbols can be retrieved in linear time by a set of $(1 + \epsilon)k$ encoded symbols, with probability of failure at most inversely polynomial in k. However, the original Raptor design does not feature the highly desirable systematic form. Further, similar to the LT codes, the constant average degree of the encoded symbols does not imply good locality.

In the same work [4], Shokrollahi provided a construction that yields a systematic flavor of Raptor codes. The Raptor encoding is not applied directly on the input symbols, rather on the output of a preprocessing step of complexity $O(k^2)$. The source symbols appear in the encoded stream, but due to the preprocessing step the parity symbols are no longer sparse in the original input symbols, despite their constant average degree.

Gummadi in his thesis [16] was the first to consider the design of Fountain codes explicitly oriented for storage applications, *i.e.*, codes that feature systematic form and efficient repair. The latter is quantified by *repair complexity*: the average number of symbol operations performed to repair a set of erased symbols. Gummadi proposes systematic variants of LT and Raptor codes that feature low (even constant) expected repair complexity. However, the overhead ϵ required for decoding is suboptimal: it cannot be made arbitrarily small.

Our main result is the analysis of the rank of a new family of sparse random matrices over $\mathbb{F}_q$. In particular, we investigate the probability that a $k \times (1 + \epsilon)k$ matrix comprising any number $0 \le s \le k$ of systematic columns and $(1 + \epsilon)k - s$ random $O(\log k)$-sparse columns has full rank. There is a long line of work on the distribution of the rank of sparse random matrices over a finite field (*e.g.*, work by Karp [17], Kovalenko [18], Balakin [19], Cooper [20] and references therein). That line of work, however, typically focuses on random matrices whose entries are independently distributed. In our case, systematic columns carry exactly one nonzero entry, while the number of nonzero entries in the remaining columns is strictly upper bounded, rendering column entries dependent.

IV. REPAIRABLE FOUNTAIN CODES

We introduce a new family of Fountain codes that are systematic and also have sparse parities. Each parity symbol is a random linear combination of up to d randomly chosen input symbols. Due to their randomized nature, our codes provide a probabilistic guarantee on successful decoding. In particular, we require that a set of $k' = (1 + \epsilon)k$ randomly selected encoded symbols, for arbitrarily small $\epsilon > 0$ can be decoded successfully with high probability, *i.e.*, with probability of failure vanishing like $1/\text{poly}(k)$. We show that under this constraint, d must be of at least logarithmic order in k, *i.e.*, $d = \Omega(\log k)$. Surprisingly, however, a logarithmic sparsity level for the parity symbols is also achievable, hence $d = \Theta(\log k)$. The sparsity of the parity columns corresponds to the *locality* of the code family. Our main result, which is asymptotic in k, is established in Theorem 1, at the end of this section. We conclude the section with a study of the *availability* of our construction.
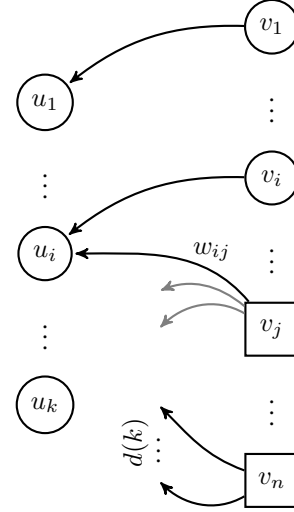

Fig. 1. Bipartite graph $G = (U, V, E)$ corresponding to our randomized code construction: U is the set of k input symbols and V is the set of n encoded symbols. The first k vertices in V have degree one and correspond to the systematic part of the encoded sequence. Each one of the remaining vertices independently and uniformly throws $d(k)$ edges, with two or more edges possibly landing on the same vertices in U.

Given a vector $\mathbf{u}$ of k input symbols in $\mathbb{F}_q$, the code is a linear mapping of $\mathbf{u}$ to a vector $\mathbf{v}$ of higher dimension n through a $k \times n$ matrix $\mathbf{G}$. The encoded sequence comprises an un-encoded copy of the k input symbols augmented by parity symbols, hence the *systematic* form. Without loss of generality, we may assume that $\mathbf{u}$ lies in the first indices of $\mathbf{v}$ followed by the parity symbols. A single parity symbol is constructed in a two step process. First, d input symbols are successively selected uniformly at random, independently, with replacement. Then, a coefficient is uniformly drawn from $\mathbb{F}_q$ for each symbol previously selected. The parity is the linear combination of the symbols selected in the first step, weighted with the coefficients drawn in the second step. The same procedure is repeated independently for subsequent parity symbols. The independent construction of parities is the hallmark of a Fountain code.

It is useful to describe our randomized construction through a correspondence to a bipartite graph $G = (U, V, E)$, depicted in Figure 1. The set U of vertices on the left side corresponds to the k input symbols, and the set V on the right corresponds to the n symbols of the encoded sequence. An edge $(u_i, v_j) \in E$ if the input symbol $u_i \in U$ is one of the symbols participating in the formation of the encoded symbol $v_j \in V$. Each of the k first vertices in V has degree equal to one and is connected to a distinct input symbol. These k vertices correspond to the deterministically constructed systematic part of the encoded sequence. Each one of the remaining vertices corresponds to a parity symbol and forms its neighborhood through the following randomized procedure. Node v_j throws an edge to a vertex in U selected uniformly at random. This step is repeated a total number of d times, independently. At the end of this process, vertex v_j has selected a subset $\mathcal{N}(v_j)$ of vertices in U, the neighborhood of v_j.

The parity symbol corresponding to vertex v_j is a random linear combination of the input symbols in its neighborhood.

Slightly abusing notation, v_j is used to denote both the vertex and the corresponding entry in the encoded sequence $\mathbf{v}$. The j-th encoded symbol can be written as

$$v_j = \sum_{i \in \mathcal{N}(v_j)} w_{ij} u_i, \qquad (1)$$

where w_{ij}'s are randomly selected uniformly and independently from $\mathbb{F}_q$. The coefficients w_{ij}'s can be embedded in the graph representation as weights on the corresponding edges. The edges of the systematic part have unit weights.

The degree of $v_j \in V$, *i.e.*, the size of its neighborhood $|\mathcal{N}(v_j)|$ can be at most equal to d, the number of edges thrown. It can be strictly smaller if a vertex in U is selected multiple times. However, when d is much smaller than k, $|\mathcal{N}(v_j)|$ will be equal to d with high probability, and a parity symbol will be a linear combination of d input symbols. To emphasize that d is allowed to grow as a function of k, we will hereafter denote it by $d(k)$.

Returning to the matrix representation, the code construction corresponds to a family of generator matrices $\mathbf{G}$ of the form $\mathbf{G} = [\ \mathbf{I}_{k \times k}\ |\ \mathbf{P}\ ]$. Every encoded symbol corresponds to a column of $\mathbf{G}$. The identity part confers the systematic form. $\mathbf{P}$, the part responsible for the construction of the parity symbols, is a random matrix whose columns are sparse, each bearing at most $d(k)$ nonzero entries. Any k encoded symbols corresponding to linearly independent columns of $\mathbf{G}$ suffice to retrieve the input $\mathbf{u}$. Conversely, reconstructing $\mathbf{u}$ from a randomly chosen set of $k' > k$ encoded symbols is possible only if k symbols among them correspond to linearly independent columns. Therefore, the key property required for successful decoding of a set $\mathcal{S}$ of k' randomly selected encoded symbols is that $\mathbf{G}_\mathcal{S}$, the $k \times k'$ matrix formed by the corresponding columns of $\mathbf{G}$, including any combination of systematic and parity parts, has full rank w.h.p.

The probability that the input can be recovered from k' randomly selected encoded symbols increases with $d(k)$. Equivalently, fewer encoded symbols suffice to attain a certain probability of successful decoding. We have highlighted the extreme case of systematic MDS codes: for the optimal guarantee that any k symbols suffice to recover the input, $d(k)$ can be no less than k. To gain further insight, note that for a set of k' encoded symbols to be successfully decoded, it is necessary that all input symbols are covered by that set. As $d(k)$ decreases, so does the probability that a particular symbol is covered by the parities in a set of k' encoded symbols, impacting the decoding guarantees.

On the other hand, as noted Section II, a systematic code with sparse parities has good locality. The relation between $d(k)$ and locality is straightforwardly quantifiable: any parity symbol v is a linear combination of at most $d(k)$ systematic symbols. Also rearranging the terms, any systematic symbol u covered by a parity v can be written as a linear combination of v and the remaining systematic symbols covered by v. Under the assumption that there exist at least one parity symbol covering every systematic symbol u, the code has locality at most $d(k)$.

In summary, decreasing $d(k)$ improves the locality of the code, with a toll on the probability of successful decoding of a random set of $k' = (1 + \epsilon)k$ encoded symbols, where ϵ is a positive constant denoting the decoding overhead. Our primary contribution, portrayed in Theorem 1, is identifying how *small* $d(k)$ can be to ensure that a randomly selected set of $k' = (1 + \epsilon)k$ symbols is decodable, or equivalently that a $k \times k'$ submatrix $\mathbf{G}_\mathcal{S}$ of $\mathbf{G}$ is full rank, with high probability.

Theorem 1. *Consider a matrix* $\mathbf{G} = [\ \mathbf{I}_{k \times k}\ |\ \mathbf{P}\ ]$, *where each column of* $\mathbf{P}$ *is independently constructed as follows:* (i) $d(k) = c \cdot \log k$ *out of the* k *entries are selected uniformly at random with replacement, and* (ii) *a value drawn uniformly at random over* $\mathbb{F}_q$ *is independently assigned to each entry selected in step* (i). *Then, for constant* $c = (8 + \rho + 2\epsilon)/\epsilon > 0$, *and* $q > k$, *a randomly selected* $k \times (1 + \epsilon)k$ *submatrix* $\mathbf{G}_\mathcal{S}$ *of* $\mathbf{G}$ *containing any number of systematic columns is full rank with probability at least* $1 - (k/q) - k^{-\rho}$.

Theorem 2 establishes a converse result stating that the *sufficient* value of $d(k)$ of Theorem 1 is order-optimal for our construction.

Theorem 2. *(Converse) If each column of* $\mathbf{P}$ *is generated independently as described with at most* $d(k)$ *nonzero entries, then* $d(k) = \Omega(\log(k))$ *is necessary for a random* $k \times k'$ *submatrix* $\mathbf{G}_\mathcal{S}$ *of* $\mathbf{G} = [\ \mathbf{I}_{k \times k}\ |\ \mathbf{P}\ ]$ *to be full rank w.h.p.*

From the two theorems, it follows that our codes achieve optimal locality with a logarithmic degree for every parity symbol. Original data is reconstructed in $O(k^3)$ using Maximum Likelihood (ML) decoding, which corresponds to solving a linear system of k' equations over $\mathbb{F}_q$. Note, however, that the Wiedemann algorithm [13] can reduce complexity to $O(k^2 \text{polylog}(k))$ on average, exploiting the sparsity of the linear equations, with negligible extra memory requirement. Finally, we note a drawback of our analysis: in order to achieve vanishingly small probability of failure as k grows, the size of the field must grow accordingly. It suffices, however, that the number of bits per symbol grows logarithmically in k: a symbol size of $(t + 1)\log k$ bits, $t > 0$, implies that $k/q = 1/k^t$.

Thus far, we have seen that our randomized construction achieves logarithmic locality: every encoded symbol belongs to at least one *local group* of cardinality $d(k) + 1$. There is a one-to-one correspondence between the local groups u belongs to and the parity symbols that cover u. Let $\mathcal{P}_u = \{v_j : k + 1 \le j \le n, u \in \mathcal{N}(v_j)\}$ be the subset of parities that cover u. Its cardinality is a binomial random variable since every generated parity independently covers u with some probability. If the total number of parities generated is rk for some constant $r > 0$, *i.e.*, proportional to the length of the input, then for $d(k) = c \log(k)$ of Theorem 1 every systematic symbol is in fact covered by a logarithmic number of parities w.h.p.

Theorem 3. *Let* rk *be the total number of parities generated, for a constant* $r > 0$, *with each parity symbol constructed as a linear combination of* $d(k) = c \log(k)$ *independently selected symbols uniformly at random with replacement. The expected number of parities covering a systematic symbol* u *is*

$$rc \log(k) - \frac{rc \log^2(k)}{k} \le E\left[|\mathcal{P}_u|\right] \le rc \log(k). \qquad (2)$$
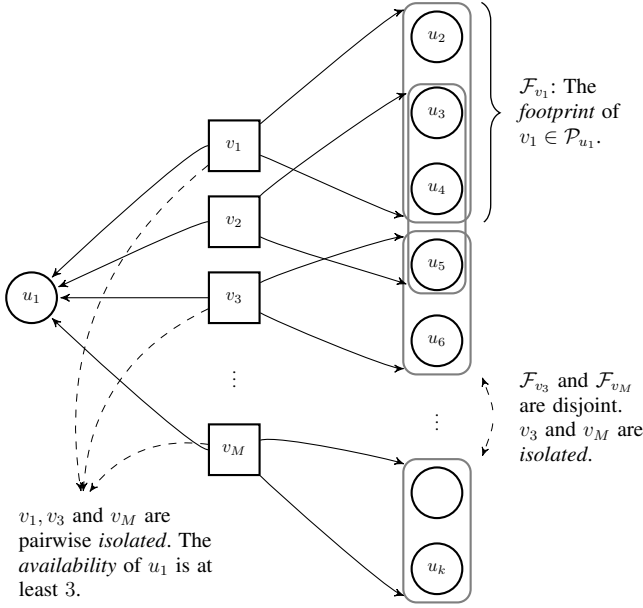
Fig. 2. The systematic symbol u_1 is covered by M parities, $v_1, \ldots, v_M$. The footprint of such a parity v_i (with respect to u_1) is the set of symbols it covers excluding u_1, *e.g.*, the footprint of v_1 is $\mathcal{F}_{v_1} = \{u_2, u_3, u_4\}$. Symbol u_1 can be reconstructed using any of the above parity symbols and its footprint. In this example, u_1 has availability at least 3 since the footprints of parities v_1, v_3, and v_M are disjoint.

Further,

$$Pr\left(\exists u : |\mathcal{P}_u| \leq (1 - \epsilon)E[|\mathcal{P}_u|]\right)$$
$$\leq \frac{1}{k^{\frac{rc\epsilon^2}{2} - 1}} \exp\left(\frac{\epsilon^2}{2} \frac{rc \log^2(k)}{k}\right). \quad (3)$$

For any ϵ, an appropriate choice of r, and c achieves a vanishing bound in (3). The above result states that with high probability all input symbols are covered by at least $(1 - \epsilon)rc\log(k)$ symbols for some $\epsilon > 0$. In the following, we will omit the constant $1 - \epsilon$ for simplicity, and assume that every systematic symbol is covered by at least $m = rc\log(k)$.

The *availability* of the input symbol u is the cardinality of the largest subset of *local groups* containing u whose only common element is u. More formally, consider a parity v_i that covers the systematic symbol u, *i.e.*, $v_i \in \mathcal{P}_u$. Then v_i is a linear combination of the symbols in $\{u\} \cup \mathcal{F}_{v_i}$, where $\mathcal{F}_{v_i}$ contains the remaining symbols covered by v_i. The set $\mathcal{F}_{v_i}$ is referred to as the *footprint* of v_i with respect to u. Note that the *footprint* of a parity symbol v_i is a concept relative to the systematic symbol u under consideration. Two parities $v_i, v_j \in \mathcal{P}_u$ are *isolated* if their footprints are disjoint. An example is depicted in Figure 2. The cardinality of the largest subset of $\mathcal{P}_u$ such that parities are pairwise isolated corresponds to the availability of the symbol u.

Under the assumption that every systematic symbol is covered by at least a logarithmic number of parities, Theorem 4 states that every systematic symbol has a logarithmic availability with high probability.

Theorem 4. *Assuming that every input symbol u is covered by at least $m = rc\log k$ parity symbols created independently as described in Section IV, for sufficiently large k, $\lambda > 0$ and*

$$\alpha > 1 - \sqrt{\lambda/rc} - \frac{\log^4 k}{k},$$

$$Pr\left(\exists u \text{ not } (\alpha m)\text{-available}\right) \leq \frac{1}{k^\lambda}. \quad (4)$$

V. A GRAPH PERSPECTIVE

The randomized construction of our erasure code is naturally mapped to a family of random bipartite graphs $G = (U, V, E)$ depicted in Figure 1. The correspondence, established early in Section IV, lays the foundation for all subsequent analysis, but also provides an alternative viewpoint for our results as purely structural properties of the random graphs, setting the coding background aside.

Under the graph perspective, Theorem 1 states that a randomly chosen subgraph of G has a perfect matching. First, consider a balanced random bipartite graph where $|U| = |V| = k$ and each vertex of V is randomly connected to $d(k) = c \log k$ nodes in U. A classical result by Erdős and Renyi [14] shows that these graphs will have perfect matchings with high probability. However, the graphs we consider are unbalanced, with $|U| = k$ and $|V| = k' = (1+\epsilon)k$ vertices, for $\epsilon \geq 0$, like the one depicted in Figure 6. Out of the k' vertices in V, s vertices are special with degree 1, corresponding to systematic symbols, and $k' - s$ are connected to $d(k) = c \log k$ vertices in U. In that sense, if we set $s = 0$ and $\epsilon = 0$ we recover the classical result of [14]. Our additional analysis is required because our proof needs to hold for all values of s ranging from 0 up to $k - 1$. This corresponds to s vertices in U being trivially matched with those vertices in V that have degree 1, and the remaining $k - s$ vertices being matched via the random edges. More formally, let $G_\mathcal{S} = (U, V_\mathcal{S}, E_\mathcal{S})$ be a subgraph of G, where $V_\mathcal{S} \subseteq V$ is a subset of k' vertices, and $E_\mathcal{S} \subseteq E$ is the subset of edges incident to $V_\mathcal{S}$. Theorem 1 states that $G_\mathcal{S}$ has a perfect matching, which for the unbalanced bipartite graph is a matching that saturates all k vertices in U. In fact, this observation is a key component in the proof of Theorem 1. The transition from the perfect matching of a subgraph to the rank of a submatrix which finalizes the proof requires only that the random coefficients are drawn from a large enough field. Along the same lines, Theorem 2 states that randomly throwing $d(k) = \Omega(\log k)$ edges on the parity symbols are necessary to guarantee that a vertex in U is connected in $G_\mathcal{S}$ with high probability.

The vertices in V, the right hand side of G, have by construction degree either equal to one or approximately equal to $d(k) = c\log(k)$ for some $c > 0$. Theorem 3 states that when $|V|$ increases linearly in $|U|$, the degree of the vertices in U is concentrated around its expectation, which is proportional to $d(k)$.

Finally, the availability of a symbol u can be mapped to the independence number of a random graph $H_u = (\mathcal{P}_u, E_u)$. $\mathcal{P}_u$ denotes the set of parities covering u, or equivalently the vertices of V in the neighborhood of u. The set of edges E_u is constructed as follows: for $v_i, v_j \in \mathcal{P}_u$, $(v_i, v_j) \in E_u$ if and only if the footprints of v_i and v_j overlap. The availability of u is the cardinality of the maximum independent set in H_u, which is shown to be at least a constant fraction of $|\mathcal{P}_u|$, and hence logarithmic in k, with high probability. Theorem 4 states that this property holds simultaneously for all $u \in U$.
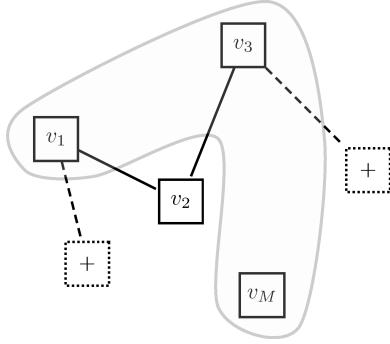
Fig. 3. Graph H_u with vertices corresponding to the parities covering u. Two parities are connected if their footprints overlap. This example is in accordance with that of Figure 2.
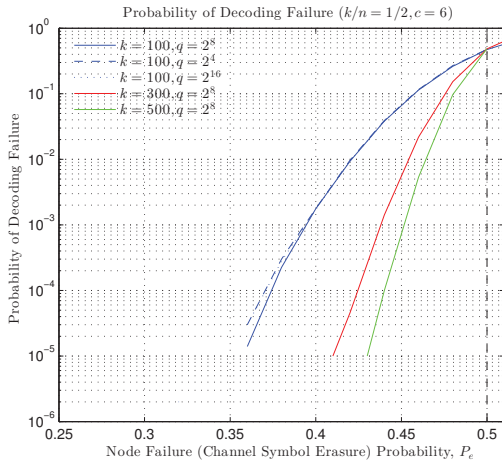

Fig. 5. Probability of decoding failure versus the decoding overhead ϵ. The probability is evaluated over multiple 10^3 randomly generated code instances with k input symbols and rate $1/2$, and 10^3 independent trials per instance. The degree of parity symbols is equal to $d(k) = \lceil c \log(k) \rceil$, with $c = 4$.

Fig. 4. Probability of decoding failure versus the probability of symbol erasure, P_e. The probability is estimated over multiple 10^3 randomly generated code instances with k input symbols and rate $1/2$, and 10^3 independent trials per instance . The degree of parity symbols is equal to $d(k) = \lceil c \log(k) \rceil$, with $c = 6$. A fixed value of P_e, corresponds to an expected decoding overhead $\overline{\epsilon} = 1 - 2P_e$.

VI. SIMULATIONS

In this section we experimentally evaluate the probability that decoding fails when a randomly selected subset of encoded symbols is available at the decoder. Since our codes are rateless, we can set any target desired rate and examine the performance under random erasures. In this experiment we set the rate equal to $1/2$; the generator matrix comprises the k columns of the identity matrix and k parity generating columns, constructed randomly and independently as described in Section IV. The degree of the parities is upper bounded by $d(k) = \lceil c \log(k) \rceil$, where the pre-log factor is arbitrarily set to a small constant value. Decoding fails exactly when the columns corresponding to the encoded symbols available to the decoder form a matrix whose rank is strictly less than k.

A first series of experiments considers a sequence of random trials in which individual encoded symbol are erased in independently with probability P_e. The ensemble of surviving symbols is available to the decoder. This corresponds to the transmission through an erasure channel with erasure probability P_e. The cardinality of the decoding set is a binomial
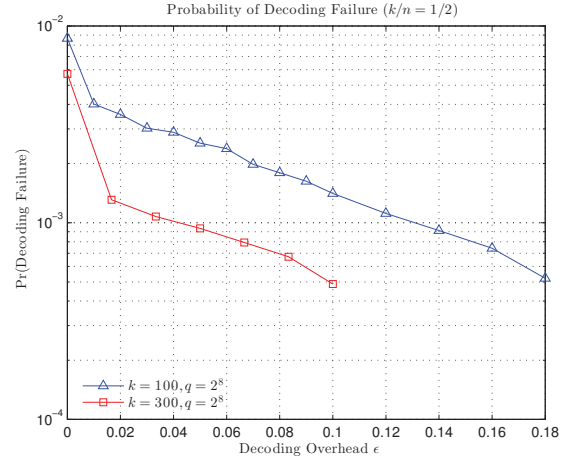
random variable with expected value equal to $(1 - P_e)2k$, which amounts to an expected decoding overhead $\overline{\epsilon} = 1 - 2P_e$. A total of 10^3 code instances are generated and each is subjected to 10^3 trials per value of P_e. Fig. 4 depicts the probability of decoding failure versus the channel erasure probability, P_e. The experiment is repeated for three values of k: $k = 100$, 300, and 500. The field size is set to $q = 2^8$, *i.e.*, a single byte per symbol, for all values of k.

In a second series of experiments, the decoding set of cardinality equal to $k' = \lceil (1 + \epsilon)k \rceil$ is selected uniformly at random in each trial from the set of $2k$ encoded symbols. Fig. 5 depicts the estimated probability of decoding failure versus the decoding overhead ϵ.

VII. ANALYSIS AND PROOFS

A. Proof of Theorem 1

Theorem 1 states that when $\mathbf{G}$ is constructed as described in section IV, a randomly selected $k \times k'$ submatrix $\mathbf{G}_{\mathcal{S}}$ is full rank w.h.p. Equivalently, there exists a set of indices $\mathcal{K} \subset \mathcal{S}$ with $|\mathcal{K}| = k$ such that $k \times k$ submatrix $\mathbf{G}_{\mathcal{K}}$ is nonsingular. More formally,

$$\Pr(\exists\, \mathcal{K} \subseteq \mathcal{S} : \det(\mathbf{G}_{\mathcal{K}}) \neq 0) = 1 - \left(\frac{k}{q} + o(1)\right). \quad (5)$$

In the following, we exploit a connection between determinants and perfect matchings (P.M.'s) in bipartite graphs. In section IV, we showed the correspondence of the randomly constructed matrix $\mathbf{G}$ to an unbalanced bipartite graph $G = (U, V, E)$. The submatrix $\mathbf{G}_{\mathcal{S}}$ corresponds to a subgraph $G_{\mathcal{S}} = (U, V_{\mathcal{S}}, E_{\mathcal{S}})$, depicted in Figure 6, where $V_{\mathcal{S}}$ is a subset of k' vertices of V, and $E_{\mathcal{S}}$ is a subset of the edges incident to vertices in $V_{\mathcal{S}}$. Similarly, a $k \times k$ submatrix $\mathbf{G}_{\mathcal{K}}$ of $\mathbf{G}_{\mathcal{S}}$ corresponds to a smaller, balanced bipartite graph, $G_{\mathcal{K}} = (U, V_{\mathcal{K}}, E_{\mathcal{K}})$, with k vertices on each side.

$\mathbf{G}_{\mathcal{K}}$ is closely related to the Edmond's matrix $\mathbf{A}_{\mathcal{K}}$ of the corresponding bipartite graph $G_{\mathcal{K}}$. By definition, the (i, j)-th
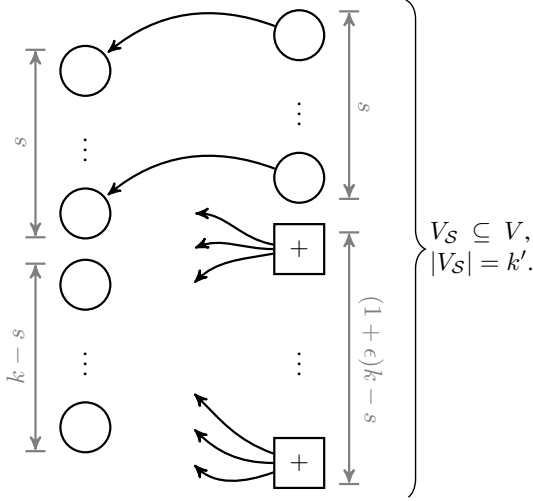
Fig. 6. Bipartite Graph $G_{\mathcal{S}} = (U, V_{\mathcal{S}}, E_{\mathcal{S}})$ corresponding to $\mathbf{G}_{\mathcal{S}}$. $V_{\mathcal{S}} \subseteq V$ consists of $k' = (1 + \epsilon)k$ vertices. Out of them s correspond systematic symbols, and $k' - s$ to parities. The graph has a perfect matching, *i.e.* a matching saturating all k vertices in U, with high probability, for any value of s.

entry of $\mathbf{A}_{\mathcal{K}}$ is

$$A_{\mathcal{K}}(i,j) = \begin{cases} a_{i,j}, & \text{if } (u_i, v_j) \in E_{\mathcal{K}} \\ 0, & \text{if } (u_i, v_j) \notin E_{\mathcal{K}} \end{cases}, \qquad (6)$$

where $u_i \in U, v_j \in V_{\mathcal{K}}$, and $a_{i,j}$'s are *indeterminates*.

Lemma 1. *The determinant of $\mathbf{A}_{\mathcal{K}}$ is nonzero if and only if there exists a perfect matching in $G_{\mathcal{K}}$, i.e.,*

$$det(\mathbf{A}_{\mathcal{K}}) \neq 0 \quad \Leftrightarrow \quad \exists \text{ P.M. in } G_{\mathcal{K}}. \qquad (7)$$

However, $\mathbf{G}_{\mathcal{K}}$ is not an actual Edmond's matrix; it is obtained from $\mathbf{A}_{\mathcal{K}}$ substituting the indeterminates with randomly drawn elements of a finite field $\mathbb{F}_q$. There are two substantially different cases in which $\det(\mathbf{G}_{\mathcal{K}}) = 0$:

- The determinant polynomial $\det(\mathbf{A}_{\mathcal{K}})$ is identically zero, which by Lemma 1 occurs if and only if $G_{\mathcal{K}}$ has no perfect matching, or
- it is not identically zero, *i.e.*, $G_{\mathcal{K}}$ has a perfect matching, but the selected coefficients correspond to a root of the polynomial.

The equivalence property in (7) is not inherited by $\mathbf{G}_{\mathcal{K}}$. In contrast to the use of indeterminates, an unfortunate selection of the random coefficients in $\mathbf{G}_{\mathcal{K}}$ can lead to zero determinant even when $G_{\mathcal{K}}$ has a perfect matching. However, if the coefficients are drawn from a sufficiently large field, the probability of this event can be driven arbitrarily low. More concretely, if $G_{\mathcal{K}}$ has a perfect matching M, then the determinant of $\mathbf{A}_{\mathcal{K}}$ is a nonzero polynomial of degree exactly k. The probability that a random assignment of coefficients from $\mathbb{F}_q$ yields a zero determinant can be upper bounded by k/q, using the Schwartz-Zippel Lemma [21]. In summary,

$$\Pr\left(\det(\mathbf{G}_{\mathcal{K}}) = 0 \mid \exists \text{ P.M. in } G_{\mathcal{K}}\right) \leq \frac{k}{q}. \qquad (8)$$

The $k \times k'$ matrix $\mathbf{G}_{\mathcal{S}}$ has $\binom{k'}{k}$ square submatrices. For successful decoding it suffices that at least one such submatrix $\hat{\mathbf{G}}_{\mathcal{K}}$ is nonsingular, *i.e.*, has nonzero determinant. In light of

(8), we ask instead whether there exists a subgraph $\hat{G}_{\mathcal{K}}$ that has a P.M.. Observe that a P.M. in a subgraph $\hat{G}_{\mathcal{K}}$ is also a P.M. in the larger graph $G_{\mathcal{S}}$. Conversely, if $G_{\mathcal{S}}$ has a perfect matching M, *i.e.*, a matching saturating all vertices in U, then such a $k \times k$ subgraph $\hat{G}_{\mathcal{K}}$ exists: its vertices are the endpoints of the edges in M. According to the following Lemma, $G_{\mathcal{S}}$ has a perfect matching M with high probability.

Lemma 2. *Consider the bipartite graph $G_{\mathcal{S}} = (U, V_{\mathcal{S}}, E_{\mathcal{S}})$ corresponding to the submatrix $\mathbf{G}_{\mathcal{S}}$ of $\mathbf{G}$. $V_{\mathcal{S}}$ contains any number s of vertices with degree 1 connected to distinct vertices in U, and $(1 + \epsilon)k - s$ vertices that have randomly thrown $d(k) = c\log(k)$ edges as described in Section IV. For appropriate constant $c \propto \rho/\epsilon$,*

$$Pr\left(\nexists \text{ P.M. in } G_{\mathcal{S}}\right) \leq 1/k^{\rho}, \qquad (9)$$

for $\rho > 0$.

The probability of equation (5) can be written as

$$\Pr(\exists \mathcal{K} \subseteq \mathcal{S} : \det(\mathbf{G}_{\mathcal{K}}) \neq 0)$$
$$= 1 - \Pr(\nexists \mathcal{K} \subseteq \mathcal{S} : \det(\mathbf{G}_{\mathcal{K}}) \neq 0)$$
$$= 1 - \left[\underbrace{\Pr(\nexists \mathcal{K} \subseteq \mathcal{S} : \det(\mathbf{G}_{\mathcal{K}}) \neq 0 | \exists M)}_{\alpha} \cdot \Pr(\exists M) \right.$$
$$\left. + \underbrace{\Pr(\nexists \mathcal{K} \subseteq \mathcal{S} : \det(\mathbf{G}_{\mathcal{K}}) \neq 0 | \nexists M)}_{\beta} \cdot \Pr(\nexists M) \right]. \quad (10)$$

As argued in the previous paragraph, the existence of M implies the existence of a subgraph $\hat{G}_{\mathcal{K}}$ that has a perfect matching. The probability $\Pr(\nexists \mathbf{G}_{\mathcal{K}} : \det(\mathbf{G}_{\mathcal{K}}) \neq 0 \mid \exists M)$, that all submatrices $\mathbf{G}_{\mathcal{K}}$ are singular despite the existence of M, is upper bounded by the probability that $\det(\hat{\mathbf{G}}_{\mathcal{K}}) = 0$, which was in turn upper bounded in (8) by k/q. Hence, $\alpha \leq k/q$. On the other hand, nonexistence of a perfect matching in $G_{\mathcal{S}}$, implies that no submatrix $\mathbf{G}_{\mathcal{K}}$ can have nonzero determinant, hence, $\beta = 1$. Continuing from (10), we have:

$$\Pr\left(\exists \mathcal{K} \subseteq \mathcal{S} : \det\left(\mathbf{G}_{\mathcal{K}}\right) \neq 0\right)$$
$$\geq 1 - \left[\frac{k}{q} \Pr\left(\exists M\right) + \Pr\left(\nexists M\right) \right]$$
$$= 1 - \frac{k}{q}\left(1 - \Pr\left(\nexists M\right)\right) - \Pr\left(\nexists M\right)$$
$$= 1 - \frac{k}{q} - \left(1 - \frac{k}{q}\right)\Pr(\nexists M). \qquad (11)$$

Finally, satisfying the conditions in Lemma 2, we can guarantee that $\Pr(\nexists M) \leq k^{-\rho}$, for $\rho > 1$. Applying the bound on the right hand side of (11), we obtain the desired result in (5). To complete the proof, it remains to prove Lemmata 1 and 2.

1) Proof of Lemma 1 - Connection between determinants and perfect matchings: We use the following expression for the determinant:

$$\det(\mathbf{A}_{\mathcal{K}}) = \sum_{\pi \in S_n} \text{sgn}(\pi) \prod_{i=1}^{n} \mathbf{A}_{\mathcal{K}}(i, \pi(i)), \qquad (12)$$

where S_n is the set of all permutations on $\{1, \ldots, n\}$, and $\text{sgn}(\pi)$ is the sign of permutation π. There is a one-to-one correspondence between a permutation $\pi \in S_n$ and a candidate perfect matching $\{(u_1, v_{\pi(1)}), \ldots, (u_n, v_{\pi(n)})\}$ in $G_{\mathcal{K}}$. Note that if the candidate P.M. does not exist in $G_{\mathcal{K}}$, *i.e.*, some edge $(u_i, v_{\pi(i)}) \notin E_{\mathcal{K}}$ then the term corresponding to π in the summation is 0. Therefore,

$$\det(\mathbf{A}_{\mathcal{K}}) = \sum_{\pi \in \mathcal{P}} \text{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)}, \tag{13}$$

where $\mathcal{P}$ is the set of perfect matchings in $G_{\mathcal{K}}$. If $\mathcal{P} = \emptyset$, *i.e.*, if $G_{\mathcal{K}}$ has no P.M., every term in the sum is equal to zero. If on the contrary $G_{\mathcal{K}}$ has a P.M., there exists a $\hat{\pi} \in \mathcal{P}$, and hence the term corresponding to $\hat{\pi}$ is $\prod_{i=1}^{n} a_{i,\hat{\pi}(i)} \neq 0$. Additionally, there is no other term in the summation containing the exact same set of variables and this term cannot be canceled out. In this case, $\det(\mathbf{A}_{\mathcal{K}}) \neq 0$, which concludes the proof of the lemma. □

2) Proof of Lemma 2: Existence of Perfect Matching in the random subgraph: We want to establish an upper bound on the probability that there is no *perfect matching (P.M.)* between U and V_S in the random $k \times k'$ bipartite graph G_S. In fact, we want to show that $d(k) = O(\log k)$ in the construction of the bipartite graph, suffices to achieve an upper bound asymptotically decaying with a rate $1/\text{poly}(k)$.

Let V_s, $0 \le |V_s| \le k$, denote the subset of V_S corresponding to systematic encoded symbols. If a P.M. exists, we may assume that all symbols in V_s participate in it. To see that, consider a vertex $v_i \in V_s$, connected to a symbol $u_i \in U$, and assume that (v_i, u_i) is *not* included in the P.M. Then, u_i must be paired with some vertex $v_j \notin V_s$, since v_i was the only systematic symbol connected to u_i. In addition, u_i is the only symbol adjacent to v_i, hence v_i does not participate in the P.M. Given such a P.M., we can construct another one substituting (u_i, v_j) with (u_i, v_i). Therefore, without loss of generality, we may assume that all vertices in V_s participate in the P.M.

Since $k' = (1 + \epsilon)k > k$, V_S contains a nonempty subset corresponding to parity symbols, denoted by $\overline{V}_s = V_S \setminus V_s$. Let U_s denote the subsets of U matched with vertices in V_s, and $\overline{U}_s = U \setminus U_s$ the remaining vertices. A P.M. between U and V_S exists if and only if a P.M. exists between $\overline{U}_s$ and $\overline{V}_s$.

The probability that a P.M. does not exist equals the probability that there exists a *contracting* set of vertices in $\overline{U}_s$, *i.e.*, a subset of $\overline{U}_s$ with a joint neighborhood smaller than its cardinality. Let $|V_s| = s$ and $|\overline{V}_s| = k' - s$. Denote by E_i the event that there exists a set of i vertices in $\overline{U}_s$ that *contracts*, *i.e.*, has at most $i - 1$ neighbors in $\overline{V}_s$. This is equivalent to at least $k' - s - (i - 1)$ vertices in $\overline{V}_s$ being only adjacent to vertices in $\overline{U}_s$ other than the i vertices of interest. Then,

$$\Pr\left(\nexists P.M. \text{ in } G_S\right) = \Pr\left(\bigcup_{i=1}^{|\overline{U}_s|} E_i\right) \le \sum_{i=1}^{|\overline{U}_s|} \Pr(E_i)$$

$$\le \sum_{i=1}^{|\overline{U}_s|} \binom{|\overline{U}_s|}{i} \binom{|\overline{V}_s|}{|\overline{V}_s| - (i-1)} \left(\frac{k-i}{k}\right)^{d(k)\left(|\overline{V}_s| - (i-1)\right)}$$

$$= \sum_{i=1}^{k-s} \binom{k-s}{i} \binom{k'-s}{k'-s-i+1} \left(\frac{k-i}{k}\right)^{d(k)\left(k'-s-i+1\right)}$$

$$= \underbrace{\sum_{i=1}^{k-s} \binom{k-s}{k-s-i} \binom{k'-s}{k'-s-i+1} \left(\frac{k-i}{k}\right)^{d(k)\left(k'-s-i+1\right)}}_{A}.$$

Lemma 3. *The binomial coefficient satisfies the well-known bound*

$$\binom{n}{k} \le 2^{nH\left(\frac{k}{n}\right)}, \tag{14}$$

where $H(p) = p\log_2 p + (1-p)\log_2(1-p)$ is the binary entropy function.

Proof. From the probability mass function of the binomial distribution with n trials and probability of success $p = \frac{k}{n} < 1$, we have

$$1 = \sum_{m=0}^{n} \binom{n}{m} p^m (1-p)^{n-m} \ge \binom{n}{k} p^k (1-p)^{n-k}$$

$$= \binom{n}{k} 2^{n[p\log_2 p + (1-p)\log_2(1-p)]} = \binom{n}{k} 2^{-nH(p)}.$$

□

Applying (14) on the coefficients of A, we obtain

$$A \le \sum_{i=1}^{k-s} 2^{[B_1(i) + B_2(i) + B_3(i)]}$$

$$\le (k-s) \max_i \left(2^{[B_1(i) + B_2(i) + B_3(i)]}\right), \tag{15}$$

where

- $B_1(i) = (k-s)H\left(\frac{k-s-i}{k-s}\right)$,
- $B_2(i) = (k'-s)H\left(\frac{k'-s-i+1}{k'-s}\right)$, and
- $B_3(i) = d(k)(k'-s-i+1)\log_2\left(\frac{k-i}{k}\right)$.

Towards our objective, it suffices to require the right hand side of (15) to vanish asymptotically faster than $1/k^\rho$, $\rho > 0$, for each value of $s \in \{0, \ldots, k\}$. Equivalently, it suffices

$$\log_2(k-s) + \sum_{l=1}^{3} B_l(i) \le -\rho \log_2(k), \tag{16}$$

for all $0 \le s \le k$ and $1 \le i \le k - s$. Expanding and rearranging terms we find that in order for (16) to hold, it suffices

$$d(k) \ge \frac{\left[\begin{array}{c} \rho\log_2(k) + 2\log_2(k-s) + \log_2(k'-s) \\ +(k-s)H\left(\frac{k-s-i}{k-s}\right) + (k'-s)H\left(\frac{k'-s-i+1}{k'-s}\right) \end{array}\right]}{-(k'-s-i+1)\log_2\left(\frac{k-i}{k}\right)}. \tag{17}$$

Our objective is now to show that the right hand side of (17) is $O(\log k)$. Let N and D denote the numerator and denominator of the right hand side of inequality (17). For the numerator N, we have the following upper bound:

$$N \le \underbrace{(3+\rho)\log_2(k) + \log_2(1+\epsilon)}_{N_1}$$

$$+ \underbrace{kH\left(\frac{k-i}{k}\right)}_{N_2} + \underbrace{(1+\epsilon)kH\left(\frac{(1+\epsilon)k-i+1}{(1+\epsilon)k}\right)}_{N_3},$$

where the inequality is due to the monotonicity of the logarithm and the fact that $g(x) = xH\left(\frac{x-y}{x}\right)$ is increasing with respect to x for $0 \le y \le x$. For the denominator D, we have:

$$D = \underbrace{(k - s - i + \epsilon k + 1)}_{\ge 0} \underbrace{\log_2\left(\frac{k}{k-i}\right)}_{\ge 0} \ge \epsilon k \log_2\left(\frac{k}{k-i}\right).$$

Recall that $\log(1 + x) > x/(x + 1)$ for $x > -1, x \ne 0$. Applying the inequality for $x = \frac{i}{k-i} > 0$, we find that D can be further lower bounded as follows

$$D \ge \epsilon k \frac{i}{k \log 2} \le \frac{\epsilon}{\log 2} i. \tag{18}$$

We examine the ratio N/D in parts.

(i) For the first part, and for $k \ge (1 + \epsilon)$ we have

$$\frac{N_1}{D} \le \frac{(3 + \rho + 1)\log_2(k)}{\epsilon k \log_2\left(\frac{k}{k-i}\right)} \le \frac{(4 + \rho)}{\epsilon} \log(k), \tag{19}$$

where for the second inequality we have used (18) and the fact that $i \ge 1$.

(ii) For the second part, expanding the entropy we have

$$\frac{N_2}{D} \le \frac{kH\left(\frac{k-i}{k}\right)}{\epsilon k \log_2\left(\frac{k}{k-i}\right)} = \frac{k-i}{\epsilon k} - \frac{\frac{i}{k}\log_2\left(\frac{i}{k}\right)}{\epsilon \log_2\left(\frac{k}{k-i}\right)}$$

$$\overset{(18)}{\le} \frac{1}{\epsilon} + \frac{1}{\epsilon}\frac{i\log_2\left(\frac{k}{i}\right)}{i/\log 2} \le \frac{2}{\epsilon}\log(k), \tag{20}$$

where the last inequality holds for $k \ge 2$.

(iii) For the third part, for $i = 1$, $N_3/D = 0$. For $i \ge 2$, first observe that $h(k) = \log\left(\frac{k}{k-i}\right)$ is decreasing in k for $0 \le i \le k$. Since $(1 + \epsilon)k > k$ and $2 \le i \le k - s$, exploiting the monotonicity of $h(k)$, we have

$$\frac{N_3}{D} \le \frac{(1 + \epsilon)kH\left(\frac{(1+\epsilon)k-i+1}{(1+\epsilon)k}\right)}{\epsilon k \log_2\left(\frac{(1+\epsilon)k}{(1+\epsilon)k-i}\right)}$$

$$\overset{(18)}{\le} \frac{(1+\epsilon)}{\epsilon}\left(1 + \frac{i-1}{(1+\epsilon)k}\frac{\log_2\frac{(1+\epsilon)k}{i-1}}{\frac{i}{(1+\epsilon)k\log 2}}\right)$$

$$\le \frac{2(1+\epsilon)}{\epsilon}\log(k), \tag{21}$$

where the last inequality holds when $k > e(1 + \epsilon)$.

Combining (19), (20) and (21), we conclude that using $d(k) = c\log(k)$, where $c = (8 + \rho + 2\epsilon)/\epsilon$, suffices to force $\Pr(\nexists \text{P.M. in } G_S) \le 1/k^\rho$, which completes the proof. $\square$

B. Proof of Theorem 2

Consider the decoding graph G_S corresponding to the $k \times k'$ submatrix $\mathbf{G}_S$ of $\mathbf{G}$. G_S is a random bipartite graph between k input and k' encoded nodes, such that each encoded node has degree at most $d(k)$.

An input symbol is *covered* by the set of k' encoded symbols, if and only if it participates with a nonzero coefficient in the formation of at least one symbol in the set. In terms of the decoding graph, an input node is covered if and only if it is adjacent to at least one encoded node.

The probability of decoding failure is lower bounded by the probability that an uncovered input node exists in G_S: all input nodes being covered is a prerequisite for the k input symbols to be retrievable from a set of k' encoded symbols.

The problem is equivalent to throwing $k' \cdot d(k)$ balls into k bins and requiring that no bin is empty with high probability. It is a standard result in balls and bins analysis that throwing $\Omega(k \log k)$ balls is necessary to that end. It is hence imperative that $k' \cdot d(k) = \Omega(k \log k)$. Taking into account that $k' = (1 + \epsilon)k$, we obtain the desired result. $\square$

C. Proof of Theorem 3

Let $\mathcal{C}_v \subseteq [k]$ be the subset of systematic symbols covered by a parity v. Also, let $\mathcal{P}_u$ be the set of parity symbols covering a systematic symbol u, and $M = |\mathcal{P}_u|$. Note that $u \in \mathcal{C}_v \Leftrightarrow v \in \mathcal{P}_u$. The total number of generated parities is rk. Hence, M is a binomial random variable with rk trials and probability of success equal to $\Pr(u \in \mathcal{C}_v)$, the probability that a parity v covers the systematic symbol u.

Every parity v throws its $d(k)$ edges uniformly at random over $[k]$, independently, with replacement. A simple union bound yields

$$\Pr(u \in \mathcal{C}_v) \le \sum_{l=1}^{d(k)}\frac{1}{k} = \frac{d(k)}{k}. \tag{22}$$

Similarly, we can obtain a lower bound:

$$\Pr(u \in \mathcal{C}_v) = 1 - \Pr(u \notin \mathcal{C}_v) = 1 - \left(1 - \frac{1}{k}\right)^{d(k)}$$

$$\ge 1 - \exp\left(-\frac{d(k)}{k}\right). \tag{23}$$

Using the fact that $\exp(x) \le 1 + x + x^2/2$ for $x \ge 0$, inequality (23) is simplified into

$$\Pr(u \in P_v) \ge \frac{d(k)}{k} - \frac{d(k)^2}{k^2}. \tag{24}$$

The probability of that parity v covers u lies in the range described by (22) and (24). Based on these bounds, we can calculate a range for the expected value of M. Taking into account that $d(k) = c\log k$, we have

$$rc\log(k) - \frac{rc\log^2(k)}{k} \le E[M] \le rc\log(k). \tag{25}$$

Since each parity is created independently, the following Chernoff bound on the lower tail of the distribution of M holds:

$$\Pr(M \le (1 - \epsilon)E[M]) \le \exp\left(-\frac{\epsilon^2}{2}E[M]\right). \tag{26}$$

The right hand side of (26) can be further bounded as follows

$$\Pr(M \le (1 - \epsilon)E[M])$$

$$\le \exp\left(-\frac{\epsilon^2}{2}\left[rc\log(k) - \frac{rc\log^2(k)}{k}\right]\right)$$

$$= \exp\left(-\log(k^{rc\epsilon^2/2})\right)\exp\left(\frac{\epsilon^2}{2}\frac{rc\log^2(k)}{k}\right)$$

$$\le \frac{1}{k^{rc\epsilon^2/2}}\exp\left(\frac{\epsilon^2 rc\log^2(k)}{2k}\right), \tag{27}$$

which is the desired result. $\square$

D. Proof of Theorem 4

Let $\mathcal{P}_u$ denote the set of parity symbols that cover systematic symbol u. We assume for simplicity that $|\mathcal{P}_u| = m = rc\log(k)$. Given that every parity was generated independently, the footprints $\mathcal{F}_v$ for $v \in \mathcal{P}_u$ are independent random variables. We are interested in the maximum cardinality subset $\mathcal{D} \subseteq \mathcal{P}_u$ such that any two parity symbols $v_i, v_j \in \mathcal{D}$ are isolated.

Consider the graph $H_u = (\mathcal{P}_u, E)$, where edge $(v_i, v_j) \in E$ if and only if v_i and v_j are not isolated. Then, $\mathcal{D}$ corresponds to the maximum independent set in H_u, $I(H_u)$. Since H_u is a random graph, its independence number $\alpha(H_u)$ is a random variable $Z = f(\mathcal{F}_{v_1}, \ldots, \mathcal{F}_{v_m})$, which is a function of the m independently drawn $\mathcal{F}_{v_i}$'s. Function $f(\cdot)$ satisfies the bounded differences condition, *i.e.*, for any configuration $\mathcal{F}_{v_1}, \ldots, \mathcal{F}_{v_m}$, substituting a single variable $\mathcal{F}_{v_i}$ with another variable $\mathcal{F}'_{v_i}$ cannot impact the function value arbitrarily. In the graph analogy, substituting $\mathcal{F}_{v_i}$ with $\mathcal{F}'_{v_i}$ for some i, corresponds to removing a vertex from H_u along with its incident edges, and inserting a new vertex arbitrarily connected to other vertices.

Lemma 4. *Consider an undirected graph $H = (V, E)$ with $|V| = M$ and let $\alpha(H)$ denote its independence number, i.e. the cardinality of the maximum independent set $I(H) \subseteq V$. Construct a graph H' as follows: remove a node v from H along with all incident edges and insert a new node v' connected to an arbitrary set of vertices in H. Then $|\alpha(H) - \alpha(H')| \leq 1$.*

Proof. Regardless of whether $v \in I(H)$ or not, the set $\mathcal{S} = I(H) \setminus \{v\}$ is common in H and H' and remains an independent set in the latter. Therefore, $\alpha(H') \geq |\mathcal{S}| \geq \alpha(H) - 1$, where equality in the second inequality holds only if $v \in I(H)$. Inversely, consider the maximum independent set in H', $I(H')$. Irrespectively of whether $v' \in I(H')$, the set $\mathcal{S}' = I(H') \setminus \{v'\}$ is an independent set in H too, implying that $\alpha(H) \geq \alpha(H') - 1$. We conclude that $-1 \leq \alpha(H) - \alpha(H') \leq 1$, which is the desired result. □

Based on the previous lemma, we have

$$\max_{\mathcal{F}_{v_1}, \ldots, \mathcal{F}_{v_m}, \mathcal{F}'_{v_i}} \left| f(\ldots, \mathcal{F}_{v_i}, \ldots) - f(\ldots, \mathcal{F}'_{v_i}, \ldots) \right| \leq 1. \quad (28)$$

Provided that $\mathcal{F}_{v_i}$'s are independent and $f(\cdot)$ satisfies condition (28), McDiarmid's inequality [22] yields

$$\Pr(Z \leq E[Z] - t) \leq \exp\left(-\frac{2t^2}{m}\right), \quad (29)$$

for $t > 0$.

The concentration result of (29) holds, even if $E[Z]$ remains unknown. A trivial lower bound on $E[Z]$ can be obtained using those vertices in H_u that are disconnected components, *i.e.*, that have degree equal to zero. Such vertices correspond to parity symbols that are isolated from all other symbols in $\mathcal{P}_u$, not only those in $\mathcal{D}$, and are always members of the maximum independent set. The probability that a parity symbol $v \in \mathcal{P}_u$ is isolated from all other symbols in $\mathcal{P}_u$ is

$$\Pr(v \text{ is isolated}) = \left(\frac{k - \left|\cup_{j=1, j \neq i}^{m-1} \mathcal{F}_{v_j}\right|}{k}\right)^{d(k)-1}$$

$$\geq \left(1 - \frac{(m-1)(d(k)-1)}{k}\right)^{d(k)-1}$$

$$= \exp\left(-\frac{(m-1)(d(k)-1)^2}{k}\right)$$

$$\geq 1 - \frac{(m-1)(d(k)-1)^2}{k}$$

$$\geq 1 - \frac{md(k)^2}{k}. \quad (30)$$

Multiplying with m, the number of symbols in $\mathcal{P}_u$, we obtain a lower bound on the expected number of completely isolated parities in $\mathcal{P}_u$, which in turn is a lower bound on $E[Z]$. In other words,

$$m - m^2\frac{d(k)^2}{k} \leq E[Z], \quad (31)$$

Therefore, we have

$$\Pr\left(Z \leq m - \frac{[md(k)]^2}{k} - t\right) \leq \Pr(Z \leq E[Z] - t).$$

Combining the above, with inequality (29), we conclude that

$$\Pr\left(Z \leq m - \frac{[md(k)]^2}{k} - t\right) \leq \exp\left(-\frac{2t^2}{m}\right). \quad (32)$$

Let $t = (1-\alpha)m - \frac{[md(k)]^2}{k}$ for some $\alpha \in (0,1)$. For sufficiently large k, t will be nonnegative. Substituting t in (32), we obtain

$$\Pr(Z \leq \alpha m) \leq \exp\left(-\frac{2\left[(1-\alpha)m - \frac{[md(k)]^2}{k}\right]^2}{m}\right). \quad (33)$$

We are interested in the value of α for which $\Pr(Z \leq \alpha m)$ decreases faster than $1/k^{1+\lambda}$, for some $\lambda > 0$. It suffices to require the right hand side of (33) is less than $1/k^{1+\lambda}$. Taking logarithms on both sides, it suffices to find α such that

$$-\frac{2\left[(1-\alpha)m - \frac{m^2 d(k)^2}{k}\right]^2}{m} \leq -(1+\lambda)\log(k)$$

$$\Leftrightarrow -2\left[\underbrace{(1-\alpha)}_{\overline{\alpha}}^2 m - \frac{m^2 d(k)^2}{k}\right]^2 \leq -(1+\lambda)m\log(k)$$

$$\Leftrightarrow \overline{\alpha}^2 m^2 - \overline{\alpha}2\frac{m^3 d(k)^2}{k} + \frac{m^4 d(k)^4}{k^2} - \frac{1+\lambda}{2}m\log(k) \geq 0.$$

The last inequality is a quadratic inequality on $\overline{\alpha}$, satisfied when

$$\overline{\alpha} \geq \frac{2\frac{m^3 d^2}{k} + \sqrt{4m^2\frac{1+\lambda}{2}m\log(k)}}{2m^2}$$

$$= \frac{md(k)^2}{k} + \sqrt{\frac{1+\lambda}{2}\frac{\log(k)}{m}}$$

$$= \frac{rc^3\log^3(k)}{k} + \sqrt{\frac{1+\lambda}{2rc}}, \quad (34)$$

which for appropriate choice of r and c, can be a solution that asymptotically lies in $(0, 1)$. Therefore, for

$$\alpha \leq 1 - \sqrt{\frac{1+\lambda}{2rc} - \frac{rc^3 \log^3(k)}{k}}, \qquad (35)$$

we have

$$\Pr\left(Z \leq \alpha \cdot m\right) \leq k^{-(1+\lambda)}. \qquad (36)$$

The probability that there exists a systematic symbol with availability lower than αm can be bounded with a union bound over all systematic symbols:

$$\Pr\left(\exists u \text{ not } (\alpha m)\text{-available}\right) \leq k \cdot k^{-(1+\lambda)} = k^{-\lambda}, \qquad (37)$$

which completes the proof. $\square$

REFERENCES

[1] M. Asteris and A. Dimakis, "Repairable fountain codes," in *Information Theory Proceedings (ISIT), 2012 IEEE International Symposium on*, 2012, pp. 1752–1756.

[2] J. W. Byers, M. Luby, M. Mitzenmacher, and A. Rege, "A digital fountain approach to reliable distribution of bulk data," *SIGCOMM Comput. Commun. Rev.*, vol. 28, pp. 56–67, October 1998.

[3] M. Luby, "LT codes," in *Proceedings of the 43rd Symposium on Foundations of Computer Science*, ser. FOCS '02. Washington, DC, USA: IEEE Computer Society, 2002, pp. 271–.

[4] A. Shokrollahi, "Raptor codes," *IEEE/ACM Trans. Netw.*, vol. 14, pp. 2551–2567, June 2006.

[5] A. G. Dimakis, P. Godfrey, Y. Wu, M. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4539 –4551, sept. 2010.

[6] M. Sathiamoorthy, M. Asteris, D. Papailiopoulos, A. G. Dimakis, R. Vadali, S. Chen, and D. Borthakur, "XORing Elephants: Novel Erasure Codes for Big Data," *Proc. VLDB Endowment*, vol. 6, no. 5, March 2013, pp. 325–336.

[7] C. Huang, H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li, and S. Yekhanin, "Erasure coding in windows azure storage," in *Proceedings of the 2012 USENIX conference on Annual Technical Conference*, ser. USENIX ATC'12. Berkeley, CA, USA: USENIX Association, 2012, pp. 2–2.

[8] O. Khan, R. Burns, J. Plank, W. Pierce, and C. Huang, "Rethinking erasure codes for cloud file systems: Minimizing i/o for recovery and degraded reads," in *Usenix Conference on File and Storage Technologies (FAST)*, 2012.

[9] F. Oggier and A. Datta, "Self-repairing homomorphic codes for distributed storage systems," in *INFOCOM, 2011 Proc. IEEE*, april 2011, pp. 1215 –1223.

[10] D. Papailiopoulos, J. Luo, A. Dimakis, C. Huang, and J. Li, "Simple regenerating codes: Network coding for cloud storage," in *INFOCOM, 2012 Proc. IEEE*, 2012, pp. 2801–2805.

[11] P. Gopalan, C. Huang, H. Simitci, and S. Yekhanin, "On the locality of codeword symbols," *IEEE Trans. Inf. Theory*, vol. 58, no. 11, pp. 6925–6934, 2012.

[12] J. Dean and L. A. Barroso, "The tail at scale," *Communications of the ACM*, vol. 56, no. 2, pp. 74–80, 2013.

[13] D. Wiedemann, "Solving sparse linear equations over finite fields," *IEEE Trans. Inf. Theory*, vol. 32, no. 1, pp. 54 – 62, January 1986.

[14] P. Erdős and A. Rényi, "On random matrices," *Publ. Math. Inst. Hungar. Acad. of Sciences. 8*, 1964.

[15] A. G. Dimakis, V. Prabhakaran, and K. Ramchandran, "Decentralized erasure codes for distributed networked storage," *IEEE/ACM Trans. Netw.*, vol. 14, pp. 2809–2816, June 2006.

[16] R. Gummadi, "Coding and scheduling in networks for erasures and broadcast," Ph.D. dissertation, University of Illinois at Urbana Champaign, 2011.

[17] J. Blömer, R. Karp, and E. Welzl, "The rank of sparse random matrices over finite fields," *Random Structures and Algorithms*, vol. 10, no. 4, pp. 407–419, 1997.

[18] I. Kovalenko, "Distribution of the linear rank of a random matrix," *Theory of Probability and Its Applications*, vol. 17, no. 2, pp. 342–346, 1973.

[19] G. Balakin, "On the distribution of the number of solutions of systems of random boolean equations," *Theory of Probability and Its Applications*, vol. 18, no. 3, pp. 598–602, 1974.

[20] C. Cooper, "On the rank of random matrices," *Random Struct. Algorithms*, vol. 16, p. 2000, 2000.

[21] R. Motwani and P. Raghavan, "Algorithms and theory of computation handbook," M. J. Atallah and M. Blanton, Eds. Chapman & Hall/CRC, 2010, ch. Randomized algorithms, pp. 12–12.

[22] C. McDiarmid, "On the method of bounded differences," in *Surveys in Combinatorics, 1989, J. Siemons ed., London Mathematical Society Lecture Note Series 141, Cambridge University Press*, 1989, pp. 148–188.

Megasthenis Asteris (S'12) is a Ph.D. student at the Department of Electrical and Computer Engineering of the University of Texas at Austin. Before that he received the M.Sc. in Electrical Engineering from the University of Southern California in 2012 and the Diploma in Electronic and Computer Engineering from the Technical University of Crete, Greece, in 2010. His research interests include coding theory with a focus on distributed storage and large-scale data processing.

Alexandros G. Dimakis (S'01 – M'09) is an Assistant Professor at the Electrical and Computer Engineering department, University of Texas at Austin. From 2009 until 2012 he was with the Viterbi School of Engineering, University of Southern California. He received his Ph.D. in 2008 and M.S. degree in 2005 in electrical engineering and computer sciences from UC Berkeley and the Diploma degree from the National Technical University of Athens in 2003. During 2009 he was a CMI postdoctoral scholar at Caltech.

He received an NSF Career award in 2011, a Google faculty research award in 2012 and the Eli Jury dissertation award in 2008. He is the co-recipient of several best paper awards including the joint Information Theory and Communications Society Best Paper Award in 2012. He is currently serving as an associate editor for IEEE Signal Processing letters. His research interests include information theory, signal processing, and networking, with a current focus on distributed storage and machine learning.