

Trivariate Lifted Codes with Disjoint Repair Groups

Nikita Polyanskii*, and Ilya Vorobyev*[†]

*Center for Computational and Data-Intensive Science and Engineering,
Skolkovo Institute of Science and Technology
Moscow, Russia 121205

[†]Advanced Combinatorics and Complex Networks Lab,
Moscow Institute of Physics and Technology
Dolgoprudny, Russia 141701

Emails: nikita.polyansky@gmail.com, vorobyev.i.v@yandex.ru

Abstract—Guo, Kopparty, and Sudan introduced the notion of lifted Reed-Solomon codes in the context of locally correctable codes. We continue the study of lifted codes with the application for so-called t -disjoint-repair-group property (t -DRGP) codes. A code is said to have the t -DRGP if every symbol in a codeword from the code has t mutually disjoint recovering sets of coordinates in the codeword. In some parameter regimes, our proposed t -DRGP codes based on lifted codes have lower redundancy than previously known t -DRGP codes.

Index Terms—Distributed storage systems, disjoint repair groups, local recovery, lifted codes

I. INTRODUCTION

Reed-Solomon codes and Reed-Muller codes are classical families of error-correcting codes which have been widely influential in coding theory, combinatorics and theoretical computer science. These codes are based on evaluations of polynomials: a codeword of one of these codes is obtained by evaluating a polynomial over a finite field \mathbb{F}_q of degree at most d at all points in \mathbb{F}_q^m . *Lifted codes* are a family of recently-introduced algebraic error-correcting codes based on evaluations of polynomials with the property that a polynomial restricted to a line in \mathbb{F}_q^m is a low-degree polynomial. This family was originally proposed by Guo, Kopparty and Sudan [1] in order to get new ranges of parameters of codes with good local correction and testing properties. The most interesting result in such lifts is a construction of high-rate codes with sub-linear time decoding. Another construction with similar features, based on *multiplicity codes*, was presented by Kopparty, Saraf and Yekhanin in [2]. Very recently, Wu [3] and Li and Wootters [4] combined both ideas in *lifted multiplicity codes*, and showed that these codes exhibit nice locality properties. More precisely, Li and Wootters discussed codes with the t -disjoint-repair-group property (t -DRGP), a notion of locality in error correcting codes. We may say that a code has the t -DRGP if any symbol of a codeword from the code can be obtained in t independent ways. Formally, let us introduce the following definition.

Definition 1. Let \mathcal{C} be a code of length N over an alphabet Σ . The code \mathcal{C} has the t -DRGP if for every $i \in [N]$, there exists t mutually disjoint sets $R_1, \dots, R_t \subset [N] \setminus \{i\}$ and functions f_1, \dots, f_t such that for all $c \in \mathcal{C}$ and for all $j \in [t]$, $f_j(c|_{R_j}) = c_i$, where $c|_R$ is the projection of c onto coordinates indexed

by R . The sets R_1, \dots, R_t will be referred to as repair groups for the i th coordinate.

A. Related work

Codes with the t -DRGP have been studied in many papers [1], [4]–[6]. We note these codes are highly relevant to so-called *one-step majority-logic decodable codes* [7]. Many other different notions related to codes with the t -DRGP have been investigated, motivated by distributed storage problems and private information retrieval and related cryptographic protocols.

When $t = o(N)$, we refer the reader to *locally repairable codes with availability* [8]–[11], which have an additional constraint on the size of recovering sets.

Codes with the t -DRGP can be seen as an instance of *private information retrieval (PIR) codes*. For the latter, we require a weaker property that every information symbol has t mutually independent recovering sets. PIR codes were suggested in [12] to decrease storage overhead in PIR schemes preserving both privacy and communication complexity. Some constructions and bounds for PIR codes can be found in [5], [12]–[15].

On the other hand, when $t = \Omega(N)$ is large, codes with t -DRGP has been investigated in the context of *locally decodable codes* and *locally correctable codes* [16], [17].

Also we mention the study of *batch codes* [5], [18], [19] which possess a more strict requirement (with respect to PIR codes), namely: each multiset of t information symbols has t mutually disjoint recovering sets from the codeword.

The quantity $k(\mathcal{C}) := \log_{|\Sigma|} |\mathcal{C}|$ will be called the *dimension* of the code \mathcal{C} . It is known [5] that the *rate*, defined as $R(\mathcal{C}) := \frac{k(\mathcal{C})}{N}$, of codes with the t -DRGP for $t = o(N)$ can approach 1 (this result follows from other papers on locally correctable codes). Therefore, it is quite natural to find the minimal *redundancy* of codes with the t -DRGP of length N which we denote by

$$r(N, t) := N \min_{\mathcal{C}} (1 - R(\mathcal{C})),$$

where the minimum is taken over all t -DRGP codes \mathcal{C} of length N . Similarly we define the optimal rate

$$R(N, t) := 1 - \frac{r(N, t)}{N}.$$

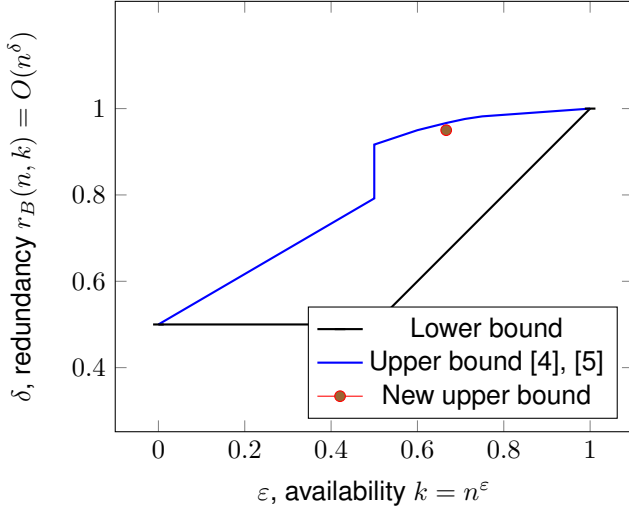


Fig. 1. Bounds on the redundancy of linear codes with the t -DRGP

Also, since for constant t , the order of the redundancy is already established $r(N, t) = \Theta(\sqrt{N})$ (e.g., see [5], [20]), we will mainly concentrate on the case when t is polynomial in N , namely: $t = N^\varepsilon$ as $N \rightarrow \infty$. Recall some known results on the minimal redundancy of linear codes with the t -DRGP for a wide range of t :

- 1) $r(N, t) \geq t - 1$;
- 2) $r(N, t) = \Omega(\sqrt{N})$ for $t \geq 2$, [14], [20];
- 3) $r(N, 2) = \sqrt{2N}(1 + o(1))$, [14];
- 4) $R(N, t) = o(1)$ for $t = \Omega(N)$, [16];
- 5) $r(N, t = N^\varepsilon) = O(N^{\varepsilon(\log_2 3 - 1) + \frac{1}{2}})$ for $0 < \varepsilon \leq \frac{1}{2}$, [4];
- 6) $r(N, t = N^\varepsilon) = O(N^{\frac{s-1}{s} + \frac{\varepsilon}{s-1}})$ for integer $s \geq 2$ and $0 < \varepsilon \leq \frac{s-1}{s}$, [5].

In particular, it follows that the best known lower bound on the redundancy of t -DRGP codes is as follows

$$r(N, t) \geq \Omega(\max(\sqrt{N}, t)). \quad (1)$$

B. Our contribution

This work continues the study of lifted codes [1], [4]. The main result of our paper is a new explicit coding construction of linear t -DRGP codes of length N with $t = N^{2/3}$ based on trivariate lifts. Up to our best knowledge this work is a first one with an analysis for trivariate polynomials in the context of the DRGP. The redundancy of our construction is

$$O(N^{\log_8(5+\sqrt{5})}) = O(N^{0.9517}).$$

Let us denote $r(N, t = N^\varepsilon) =: O(N^\delta)$. The lower bound given by (1) along with old and new upper bounds on $\delta = \delta(\varepsilon)$ are plotted in Figure 1. The existence result of our work shows that the known upper bound on $\delta(\varepsilon)$ can be improved for $\varepsilon \in (0.6053, 2/3]$.

C. Outline

The remainder of the paper is organized as follows. In Section II, we introduce all the necessary results, definitions and

notation. Section III discusses trivariate lifted codes with the disjoint-repair-group property. Finally, Section IV concludes the paper.

II. PRELIMINARIES

In this section we introduce the background and notation we will use throughout the next section.

Similarly to [1], [4], the following statement turns out to be useful for our analysis.

Lemma 1 (Lucas's Lemma). *For non-negative integers m and n and a prime p , the following arithmetic relation holds:*

$$\binom{m}{n} \equiv \prod_{i=0}^{\ell-1} \binom{m_i}{n_i} \pmod{p},$$

where

$$m = m_{\ell-1}p^{\ell-1} + m_{\ell-2}p^{\ell-2} + \cdots + m_1p + m_0,$$

and

$$n = n_{\ell-1}p^{\ell-1} + n_{\ell-2}p^{\ell-2} + \cdots + n_1p + n_0$$

are the base p expansions of m and n , respectively.

Remark 1. In fact, we will apply a particular case of this lemma when $p = 2$. We write $n \leq_2 m$ if $m_i \geq n_i$ for all $i \in \{0, 1, \dots, \ell-1\}$, where m_i and n_i are the i th digits in the binary expansions of m and n , respectively. So, Lucas's lemma states that $\binom{m}{n} \equiv 1 \pmod{2}$ iff $n \leq_2 m$.

A. Good polynomials

First of all, let \mathbb{F}_q denote the finite field of order q with characteristic 2, i.e., $q = 2^m$. Let $\mathbb{F}_q[x_1, \dots, x_s]$ be the ring of polynomials in the variables x_1, \dots, x_s with coefficients in \mathbb{F}_q . We say that two polynomials f and g from $\mathbb{F}_q[x_1, \dots, x_s]$ are *equivalent* if $f(a_1, \dots, a_s) = g(a_1, \dots, a_s)$ for all $a_1, \dots, a_s \in \mathbb{F}_q$. We note that since $a^q - a = 0$ for all $a \in \mathbb{F}_q$, an arbitrary univariate polynomial is equivalent to the polynomial of degree at most $q-1$. Similarly, any monomial $x_1^{i_1} \dots x_s^{i_s}$ is equivalent to the monomial $x_1^{i'_1} \dots x_s^{i'_s}$, where $i'_j = i_j$ if $i_j < q$, or $i'_j - 1$ is the residue of $i_j - 1$ modulo $q-1$, otherwise.

Let us define a set of lines we will use for constructing recovering sets

$$\mathcal{L}(q, s) := \{(t, a_2t + b_2, \dots, a_st + b_s) \mid t \in \mathbb{F}_q : a_i, b_j \in \mathbb{F}_q\}.$$

We say that polynomial $f \in \mathbb{F}_q[x_1, \dots, x_s]$ is *d-good* if for any line $(l(t))_{t \in \mathbb{F}_q}$ from the family $\mathcal{L}(q, s)$, the univariate polynomial $f(l(t))$ is equivalent to the polynomial of degree at most d .

B. Span of good monomials

In fact, it is quite complicated to deal with the definition of good polynomials. To make our analysis simpler, we will work with good monomials only.

Let us consider the set $\mathcal{M}(q, s, d)$ consisting of monomials $x_1^{i_1} \dots x_s^{i_s}$ such that $x_1^{i_1} \dots x_s^{i_s}$ is d -good and $0 \leq i_j < q$ for

all $j \in [s]$. Note that all the monomials are independent over \mathbb{F}_q . Define the family $\mathcal{F}(q, s, d)$ of polynomials spanned by the monomials from $\mathcal{M}(q, s, d)$.

C. Lifted codes

Let us define the standard evaluation map

$$e(f) : \mathbb{F}_q[x_1, \dots, x_s] \rightarrow \mathbb{F}_q^s$$

in the following manner

$$e(f) = (f(x_1, \dots, x_s))|_{(x_1, \dots, x_s) \in \mathbb{F}_q^s}$$

Now we are in a good position to give a key definition of lifted codes.

Definition 2. The (q, s, d) lifted code is a code \mathcal{C} over alphabet $\Sigma = \mathbb{F}_q$ of length q^s with dimension $|\mathcal{M}(q, s, d)|$ defined as follows

$$\mathcal{C} := \{e(f) : f \in \mathcal{F}(q, s, d)\}.$$

Reed-Solomon codes illustrate a good example of univariate lifted codes of length q and dimension $d + 1$. Bivariate lifted codes have been investigated in several papers [1], [4], [6].

III. TRIVARIATE LIFTED CODES WITH THE DRGP

In this section, we restrict ourselves for considering trivariate lifts only. The main statement of this paper is given below.

Theorem 2. Let $q = 2^\ell$. The $(q, 3, q - 2)$ lifted code \mathcal{C} is a code over alphabet \mathbb{F}_q with the following properties:

- 1) The length of the code is q^3 .
- 2) The redundancy of the code is at most

$$r(\mathcal{C}) = O\left(\left(5 + \sqrt{5}\right)^\ell\right).$$

- 3) The code has the q^2 -DRGP.

This statement immediately implies the following bound on the redundancy of codes with the t -DRGP.

Corollary 1. The minimal redundancy of $N^{2/3}$ -DRGP codes of length N is bounded as follows

$$r(N, N^{2/3}) = O\left(N^{\log_8(5 + \sqrt{5})}\right) = O\left(N^{0.9517}\right).$$

Proof of Theorem 2. The first property follows from the fact that the number of evaluation points is $|\mathbb{F}_q^3| = q^3$. To prove the last property, we note that the restriction of a polynomial f from the family $\mathcal{F}(q, 3, q - 2)$ to a line of the form $(t, \alpha t + \beta, \gamma t + \delta)$ is equivalent to a univariate polynomial of degree at most $q - 2$. Let x be some point from \mathbb{F}_q^3 which lies on some line l from $\mathcal{L}(q, 3)$. To recover symbol $f(x)$, it is sufficient to read all other symbols on the line l . Based on $q - 1$ points one needs to interpolate a univariate polynomial of degree at most $q - 2$ by Lagrange's method. After that, we evaluate the polynomial in the required point. Since for any point x in \mathbb{F}_q^3 , there are q^2 mutually disjoint (except the point x itself) lines from $\mathcal{L}(q, 3)$ containing x , we have q^2 mutually disjoint recovering sets for symbol $f(x)$, where f is from family $\mathcal{F}(q, 3, q - 2)$.

Finally let us focus on the second property. To estimate the redundancy of the lifted code, we need to bound the number of d -good monomials. A monomial $x_1^a x_2^b x_3^c$ is d -good if for every α, β, γ and δ from \mathbb{F}_q , the univariate polynomial

$$\begin{aligned} g(u) &:= g_0 + g_1 u + \dots + g_{3q-3} u^{3q-3} = u^a (\alpha u + \beta)^b (\gamma u + \delta)^c \\ &= \sum_{i=0}^b \sum_{j=0}^c \alpha^i \beta^{b-i} \gamma^j \delta^{c-j} \binom{b}{i} \binom{c}{j} u^{a+i+j}. \end{aligned}$$

can be represented as a polynomial of degree at most $q - 2$. Now we observe that $g(u)$ is equivalent to the unique polynomial $h(u)$ of degree at most $q - 1$, i.e., $h(u) = h_0 + h_1 u + \dots + h_{q-1} u^{q-1}$. Indeed, it suffices to subtract an appropriate multiple of $u^q - u$ from $g(u)$. Moreover, the coefficient of u^{q-1} in $h(u)$ can be computed as follows

$$h_{q-1} = g_{q-1} + g_{2q-2} + g_{3q-3}.$$

We remark that three conditions $g_{q-1} = 0$, $g_{2q-2} = 0$ and $g_{3q-3} = 0$ guarantee the property $h_{q-1} = 0$. If we have $a + b + c < 3q - 3$, then $g_{3q-3} = 0$.

Now let us concentrate on the coefficient g_{q-1} . Note that $g_{q-1} = 0$ if $\binom{b}{i} \binom{c}{j} = 0$ for all non-negative i and j such that $i + j = a^*$, where $a^* = q - 1 - a$.

Lemma 3. Let $q = 2^\ell$. By $s_0(\ell)$ denote the number of distinct integer triples (a, b, c) with the properties

- 1) $0 \leq a < q$, $0 \leq b < q$, $0 \leq c < q$,
- 2) there exist non-negative integers i and j such that $i + j = a$ and $\binom{b}{i} \binom{c}{j} \neq 0$ in \mathbb{F}_q .

Then $s_0(\ell)$ satisfies the following asymptotic inequality

$$s_0(\ell) = O\left(\left(5 + \sqrt{5}\right)^\ell\right), \quad \ell \rightarrow \infty.$$

Proof of Lemma 3. By $S_0(\ell)$ denote the set of triples (a, b, c) satisfying the properties described in the statement of the lemma. By $S_1(\ell)$ denote the set of triples (a, b, c) satisfying

$$1^*) \quad q \leq a < 2q - 1, \quad 0 \leq b < q, \quad 0 \leq c < q$$

and the second property from the statement. Define $s_0(\ell) := |S_0(\ell)|$ and $s_1(\ell) := |S_1(\ell)|$. It remains to estimate the asymptotics of $s_0(\ell)$ as $\ell \rightarrow \infty$. For this purpose, we shall prove two recurrent inequalities on s_0 and s_1 :

$$s_0(\ell) \leq 7s_0(\ell - 1) + s_1(\ell - 1), \quad (2)$$

$$s_1(\ell) \leq s_0(\ell - 1) + 3s_1(\ell - 1). \quad (3)$$

For $(a, b, c) \in S_0(\ell)$ or $(a, b, c) \in S_1(\ell)$, there exist non-negative integers i and j such that $i + j = a$ and $\binom{b}{i} \binom{c}{j} \neq 0$ in \mathbb{F}_q . By Remark 1 we know $\binom{b}{i} \binom{c}{j}$ could be non-zero in only the case when both conditions $i \leq_2 b$ and $j \leq_2 c$ hold true.

Let us consider the binary expansions of a , b , c , and some (of possibly many) i and j :

$$\begin{aligned} a &= a_0 + a_1 2 + \dots + a_k 2^k + \dots + a_{\ell-1} 2^{\ell-1} + a_\ell 2^\ell, \\ b &= b_0 + b_1 2 + \dots + b_k 2^k + \dots + b_{\ell-1} 2^{\ell-1}, \\ c &= c_0 + c_1 2 + \dots + c_k 2^k + \dots + c_{\ell-1} 2^{\ell-1}, \\ i &= i_0 + i_1 2 + \dots + i_k 2^k + \dots + i_{\ell-1} 2^{\ell-1}, \\ j &= j_0 + j_1 2 + \dots + j_k 2^k + \dots + j_{\ell-1} 2^{\ell-1}. \end{aligned}$$

We observe that $a_\ell = 0$ and $a_\ell = 1$ if $(a, b, c) \in S_0(\ell)$ and $(a, b, c) \in S_1(\ell)$, respectively. Now we define $b' := b - b_{\ell-1} 2^{\ell-1}$, $c' := c - c_{\ell-1} 2^{\ell-1}$, $i' := i - i_{\ell-1} 2^{\ell-1}$ and $j' := j - j_{\ell-1} 2^{\ell-1}$. Let $a' := i' + j'$.

Suppose $(a, b, c) \in S_0(\ell)$. There are two possible cases $(a', b', c') \in S_0(\ell-1)$ and $(a', b', c') \in S_1(\ell-1)$. Let us construct 7 maps $\phi_1, \dots, \phi_7 : S_0(\ell-1) \rightarrow S_0(\ell)$ as follows $\phi_k((a', b', c')) = (a, b, c)$, where a, b, c and the corresponding values i, j are specified in Table I. Additionally, we determine a map $\phi_8 : S_1(\ell-1) \rightarrow S_0(\ell)$. All the elements from $S_0(\ell)$ are covered by the images of $\{\phi_1, \phi_2, \dots, \phi_8\}$.

I. Indeed, if $(a, b, c) \in S_0(\ell)$ and $(a', b', c') \in S_0(\ell-1)$, then

$$\begin{aligned} (a, b, c) &= \phi_1((a', b', c')), & \text{if } a_{\ell-1} = 0, b_{\ell-1} = 0, c_{\ell-1} = 0, \\ (a, b, c) &= \phi_2((a', b', c')), & \text{if } a_{\ell-1} = 0, b_{\ell-1} = 1, c_{\ell-1} = 0, \\ (a, b, c) &= \phi_3((a', b', c')), & \text{if } a_{\ell-1} = 0, b_{\ell-1} = 0, c_{\ell-1} = 1, \\ (a, b, c) &= \phi_4((a', b', c')), & \text{if } a_{\ell-1} = 0, b_{\ell-1} = 1, c_{\ell-1} = 1, \\ (a, b, c) &= \phi_5((a', b', c')), & \text{if } a_{\ell-1} = 1, b_{\ell-1} = 1, c_{\ell-1} = 0, \\ (a, b, c) &= \phi_6((a', b', c')), & \text{if } a_{\ell-1} = 1, b_{\ell-1} = 0, c_{\ell-1} = 1, \\ (a, b, c) &= \phi_7((a', b', c')), & \text{if } a_{\ell-1} = 1, b_{\ell-1} = 1, c_{\ell-1} = 1. \end{aligned}$$

II. If $(a, b, c) \in S_0(\ell)$ and $(a', b', c') \in S_1(\ell-1)$, then it means that $a_{\ell-1} = 1$. Now we need to carry out a more careful analysis. First of all, $(a, b, c) = \phi_8((a', b', c'))$ if $a_{\ell-1} = 1, b_{\ell-1} = 0, c_{\ell-1} = 0$. In all the remaining cases we need to apply the following evident claim proved in Appendix.

Proposition 1. If $(a, b, c) \in S_1(\ell)$, then $(a - 2^\ell, b, c) \in S_0(\ell)$.

This proposition implies that $(a' - 2^{\ell-1}, b', c') \in S_0(\ell-1)$. Therefore,

$$(a, b, c) = \begin{cases} \phi_5((a' - 2^{\ell-1}, b', c')), & \text{if } b_{\ell-1} = 1, c_{\ell-1} = 0, \\ \phi_6((a' - 2^{\ell-1}, b', c')), & \text{if } b_{\ell-1} = 0, c_{\ell-1} = 1, \\ \phi_7((a' - 2^{\ell-1}, b', c')), & \text{if } b_{\ell-1} = 1, c_{\ell-1} = 1. \end{cases}$$

Cases **I** and **II** prove (2).

Now suppose $(a, b, c) \in S_1(\ell)$. There are two possible cases $(a', b', c') \in S_0(\ell-1)$ and $(a', b', c') \in S_1(\ell-1)$. Let us define a map $\phi_9 : S_0(\ell-1) \rightarrow S_1(\ell)$ and 3 maps $\phi_{10}, \phi_{11}, \phi_{12} : S_1(\ell-1) \rightarrow S_1(\ell)$ according to Table I. Let us prove that all the elements from $S_1(\ell)$ are covered by the images of $\{\phi_9, \phi_{10}, \phi_{11}, \phi_{12}\}$.

III. Indeed, if $(a, b, c) \in S_1(\ell)$ and $(a', b', c') \in S_0(\ell-1)$, then it follows that $a_\ell = 1, a_{\ell-1} = 0$. Therefore, $b_{\ell-1} = 1$ and $c_{\ell-1} = 1$ and $(a, b, c) = \phi_9((a', b', c'))$.

TABLE I
TRIPLES (a, b, c) DETERMINING MAPS ϕ_1, \dots, ϕ_{12}

k	a	b	c	i	j
1	a'	b'	c'	i'	j'
2	a'	$b' + 2^{\ell-1}$	c'	i'	j'
3	a'	b'	$c' + 2^{\ell-1}$	i'	j'
4	a'	$b' + 2^{\ell-1}$	$c' + 2^{\ell-1}$	i'	j'
5	$a' + 2^{\ell-1}$	$b' + 2^{\ell-1}$	c'	$i' + 2^{\ell-1}$	j'
6	$a' + 2^{\ell-1}$	b'	$c' + 2^{\ell-1}$	i'	$j' + 2^{\ell-1}$
7	$a' + 2^{\ell-1}$	$b' + 2^{\ell-1}$	$c' + 2^{\ell-1}$	$i' + 2^{\ell-1}$	j'
8	a'	b'	c'	i'	j'
9	$a' + 2^\ell$	$b' + 2^{\ell-1}$	$c' + 2^{\ell-1}$	$i' + 2^{\ell-1}$	$j' + 2^{\ell-1}$
10	$a' + 2^{\ell-1}$	$b' + 2^{\ell-1}$	c'	$i' + 2^{\ell-1}$	j'
11	$a' + 2^{\ell-1}$	b'	$c' + 2^{\ell-1}$	i'	$j' + 2^{\ell-1}$
12	$a' + 2^\ell$	$b' + 2^{\ell-1}$	$c' + 2^{\ell-1}$	$i' + 2^{\ell-1}$	$j' + 2^{\ell-1}$

IV. If $(a, b, c) \in S_1(\ell)$ and $(a', b', c') \in S_1(\ell-1)$, then we have

$$(a, b, c) = \begin{cases} \phi_{10}((a', b', c')), & \text{if } b_{\ell-1} = 1, c_{\ell-1} = 0, \\ \phi_{11}((a', b', c')), & \text{if } b_{\ell-1} = 0, c_{\ell-1} = 1, \\ \phi_{12}((a', b', c')), & \text{if } b_{\ell-1} = 1, c_{\ell-1} = 1. \end{cases}$$

Cases **III** and **IV** imply (3).

Now let us compute a bound on the asymptotics of $s_0(\ell)$ as $\ell \rightarrow \infty$. To this end, we introduce two equations:

$$\begin{aligned} q_0(\ell) &= 7q_0(\ell-1) + q_1(\ell-1), \\ q_1(\ell) &= q_0(\ell-1) + 3q_1(\ell-1). \end{aligned}$$

If $\{q_0, q_1\}$ satisfies the same starting conditions as $\{s_0, s_1\}$, i.e., $q_0(1) = s_0(1)$ and $q_1(1) = s_1(1)$, then we have $q_0(\ell) \geq s_0(\ell)$ and $q_1(\ell) \geq s_1(\ell)$ for all $\ell \geq 1$. From two equations on q_0 and q_1 we conclude that

$$q_1(\ell+1) - 3q_1(\ell) = 7q_1(\ell) - 21q_1(\ell-1) + q_1(\ell-1).$$

The roots of the equation

$$x^2 - 10x + 20 = 0$$

are

$$x_1 = 5 + \sqrt{5}, \quad x_2 = 5 - \sqrt{5}.$$

Therefore, we have

$$s_0(\ell) \leq q_0(\ell) = O((5 + \sqrt{5})^\ell).$$

Lemma 3 is proved. \square

Lemma 3 claims that the number of triples (a, b, c) with possibly non-zero coefficient g_{q-1} is $O((5 + \sqrt{5})^\ell)$.

Now let us focus on the coefficient g_{2q-2} . Note that $g_{2q-2} = 0$ if $\binom{b}{i} \binom{c}{j} = 0$ for all non-negative i and j such that $i+j = a^*$, where $a^* = 2q - 2 - a$. Even if we allow a^* to be between 0 and $2q - 1$, following the proof of Lemma 3, one can be easily check that the number of triples (a, b, c) , for which the coefficient g_{2q-2} could be non-zero, satisfies the same upper bound as g_{q-1} .

Therefore, the number of d -good monomials over \mathbb{F}_q with $q = 2^\ell$ is at least $8^\ell - c(5 + \sqrt{5})^\ell$ for some constant c . In other words, the redundancy of the lifted code is $O((5 + \sqrt{5})^\ell)$. This completes the proof of Theorem 2. \square

IV. CONCLUSION

In this paper we presented a two-fold result. First, a new explicit coding construction of linear codes with t -DRGP based on trivariate lifts was developed. Second, our construction improves the redundancy of previously known t -DRGP code of length N , where $t \in (N^{0.6053}, N^{2/3}]$.

There are several directions for future research on t -DRGP codes. First, the natural open question arose in this work is to construct multiplicity trivariate lifted codes which would improve the redundancy of t -DRGP codes in a wide range of t . Second, it is of great interest to improve the lower bound on the redundancy given by inequality (1).

ACKNOWLEDGMENT

This research was supported by a grant from the Russian Science Foundation (grant no. 19-71-00137).

REFERENCES

- [1] A. Guo, S. Kopparty, and M. Sudan, "New affine-invariant codes from lifting," in *Proceedings of the 4th conference on Innovations in Theoretical Computer Science*. ACM, 2013, pp. 529–540.
- [2] S. Kopparty, S. Saraf, and S. Yekhanin, "High-rate codes with sublinear-time decoding," *Journal of the ACM (JACM)*, vol. 61, no. 5, p. 28, 2014.
- [3] L. Wu, "Revisiting the multiplicity codes: A new class of high-rate locally correctable codes," in *2015 53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. IEEE, 2015, pp. 509–513.
- [4] R. Li and M. Wootters, "Lifted multiplicity codes," *arXiv preprint arXiv:1905.02270*, 2019.
- [5] H. Asi and E. Yaakobi, "Nearly optimal constructions of pir and batch codes," *IEEE Transactions on Information Theory*, 2018.
- [6] S. L. Frank-Fischer, V. Guruswami, and M. Wootters, "Locality via partially lifted codes," *arXiv preprint arXiv:1704.08627*, 2017.
- [7] S. Lin and D. J. Costello, *Error control coding*. Pearson Education India, 2001.
- [8] A. Wang, Z. Zhang, and M. Liu, "Achieving arbitrary locality and availability in binary codes," in *Information Theory (ISIT), 2015 IEEE International Symposium on*. IEEE, 2015, pp. 1866–1870.
- [9] L. Pamies-Juarez, H. D. Hollmann, and F. Oggier, "Locally repairable codes with multiple repair alternatives," *arXiv preprint arXiv:1302.5518*, 2013.
- [10] A. S. Rawat, D. S. Papailiopoulos, A. G. Dimakis, and S. Vishwanath, "Locality and availability in distributed storage," *IEEE Transactions on Information Theory*, vol. 62, no. 8, pp. 4481–4493, 2016.
- [11] I. Tamo and A. Barg, "Bounds on locally recoverable codes with multiple recovering sets," in *2014 IEEE International Symposium on Information Theory*. IEEE, 2014, pp. 691–695.
- [12] A. Fazeli, A. Vardy, and E. Yaakobi, "Pir with low storage overhead: coding instead of replication," *arXiv preprint arXiv:1505.06241*, 2015.
- [13] S. R. Blackburn and T. Etzion, "Pir array codes with optimal pir rates," in *Information Theory (ISIT), 2017 IEEE International Symposium on*. IEEE, 2017, pp. 2658–2662.
- [14] S. Rao and A. Vardy, "Lower bound on the redundancy of pir codes," *arXiv preprint arXiv:1605.01869*, 2016.
- [15] Y. Zhang, X. Wang, H. Wei, and G. Ge, "On private information retrieval array codes," *arXiv preprint arXiv:1609.09167*, 2016.
- [16] D. P. Woodruff, "A quadratic lower bound for three-query linear locally decodable codes over any field," *Journal of Computer Science and Technology*, vol. 27, no. 4, pp. 678–686, 2012.
- [17] J. Katz and L. Trevisan, "On the efficiency of local decoding procedures for error-correcting codes," in *STOC*. Citeseer, 2000, pp. 80–86.

Algorithm 1 Computing i' and j'

Input: integers i, j and ℓ such that $i + j \geq 2^\ell$, $i < 2^\ell$, $j < 2^\ell$
Output: integers i' and j' such that $i' + j' = i + j - 2^\ell$, $i' \leq_2 i$ and $j' \leq_2 j$
Initialisation :
 $i' := i, j' := j$ and $k := \ell$
while $i'_{k-1} + j'_{k-1} = 1$ **do**
 $i' := i' - 2^{k-1}i'_{k-1}, \quad j' := j' - 2^{k-1}j'_{k-1}, \quad k := k - 1$
end while
 $i' := i' - 2^{k-1}$ and $j' := j' - 2^{k-1}$
return i' and j'

- [18] Y. Ishai, E. Kushilevitz, R. Ostrovsky, and A. Sahai, "Batch codes and their applications," in *Proceedings of the thirty-sixth annual ACM symposium on Theory of computing*. ACM, 2004, pp. 262–271.
- [19] N. Polyanskii and I. Vorobyev, "Constructions of batch codes via finite geometry," *arXiv*, 2019.
- [20] M. Wootters, "Linear codes with disjoint repair groups," *personal communication*, 2016.

APPENDIX

A. Proof of Proposition 1

Let $(a, b, c) \in S_1(\ell)$. This means that $2^\ell \leq a \leq 2^{\ell+1} - 1$ and there exist non-negative integers i and j such that $i + j = a$, $i \leq_2 b$ and $j \leq_2 c$. Now we shall find integers i' and j' such that $i' + j' = a - 2^\ell$, $i' \leq_2 i$ and $j' \leq_2 j$. It would immediately imply that $(a - 2^\ell, b, c) \in S_0(\ell)$.

Let the binary expansions of i and j be as follows

$$i = i_0 + i_1 2 + \dots + i_k 2^k + \dots + i_{\ell-1} 2^{\ell-1},$$

$$j = j_0 + j_1 2 + \dots + j_k 2^k + \dots + j_{\ell-1} 2^{\ell-1}.$$

We will define i' and j' by the inductive procedure depicted as Algorithm 1. One can easily see that after each iteration in the "while" loop we obtain new i' and j' such that $i' \leq_2 i$ and $j' \leq_2 j$. The property $i' + j' = a - 2^\ell$ follows from the facts that we decrease the total sum $i' + j'$ by 2^{k-1} after one step in the "while" loop and the total sum is decreased by 2^k at the final step of the procedure. Therefore, the difference between $i + j$ and $i' + j'$ is $2^{\ell-1} + 2^{\ell-2} + \dots + 2^k + 2^k = 2^\ell$.