Advance Access publication on 22 September 2021 https://doi.org/10.1093/comjnl/bxab121

On the Modulus in Matching Vector Codes

LIN ZHU, WEN MING LI AND LIANG FENG ZHANG*

School of Information Science and Technology, ShanghaiTech University, Shanghai 201210, China
**Corresponding author: zhanglf@shanghaitech.edu.cn*

A k-query locally decodable code (LDC) C allows one to encode any n-symbol message x as a codeword $C(x)$ of N symbols such that each symbol of x can be recovered by looking at k symbols of $C(x)$, even if a constant fraction of $C(x)$ has been corrupted. Currently, the best known LDCs are matching vector codes (MVCs). A modulus $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ may result in an MVC with $k \leq 2^r$ and $N = \exp(\exp(O((\log n)^{1-1/r}(\log\log n)^{1/r})))$. The m is *good* if it is possible to have $k < 2^r$. The good numbers yield more efficient MVCs. Prior to this work, there are only *finitely many* good numbers. All of them were obtained via computer search and have the form $m = p_1 p_2$. In this paper, we study good numbers of the form $m = p_1^{\alpha_1} p_2^{\alpha_2}$. We show that if $m = p_1^{\alpha_1} p_2^{\alpha_2}$ is good, then any multiple of m of the form $p_1^{\beta_1} p_2^{\beta_2}$ must be good as well. Given a good number $m = p_1^{\alpha_1} p_2^{\alpha_2}$, we show an explicit method of obtaining smaller good numbers that have the same prime divisors. Our approach yields *infinitely many* new good numbers.

Keywords: matching vector codes; locally decodable codes; private information retrieval

Received 2 October 2020; Revised 9 June 2021; Editorial Decision 20 July 2021
Handling editor: Dirk Sudholt

1. INTRODUCTION

Classical error-correcting codes allow one to encode any n-bit message x as an N-bit codeword $C(x)$ such that x can still be recovered, even if a constant fraction of $C(x)$ has been corrupted. The disadvantage of such codes is that one has to read all or most of the codeword to recover any information about x. As a better solution for decoding particular bits of the message, a (k, δ, ϵ)-*locally decodable code* (LDC) [1] encodes any n-bit message x to an N-bit codeword, such that any message bit x_i can be recovered with probability $\geq 1 - \epsilon$, by a randomized decoding procedure that makes at most k queries, even if δN bits of $C(x)$ have been corrupted. Such codes have interesting applications [2, 3] in cryptography and complexity theory. For an efficient LDC, both the code *length* N and the *query complexity* k should be as small as possible, as functions of n.

Following [1, 4, 5], Gasarch [2] and Goldreich *et al.* [4] conjectured that for any constant k, the length N of a k-query LDC should be $\exp(n^{\Omega(1)})$. Yekhanin [6] disproved this conjecture with a three-query LDC of length $\exp(\exp(O(\log n/\log\log n)))$, assuming that there are infinitely many Mersenne primes. For any $r \geq 2$, Efremenko [7] provided a construction of 2^r-query LDCs of length $N_r = \exp(\exp(O((\log n)^{1-1/r}(\log\log n)^{1/r})))$ under no assumptions, and in particular a three-query LDC when $r = 2$. Such codes have been reformulated and called *matching vector codes* (MVCs) in [8].

The MVCs in [7] are based on two ingredients: S-matching family and S-decoding polynomial. For $r \geq 2$, let $\mathcal{M}_r$ be the set of integers of the form $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where $p_1, p_2, \ldots, p_r > 2$ are distinct primes and $\alpha_1, \alpha_2, \ldots, \alpha_r > 0$. The existence of both ingredients in MVCs depends on a *modulus* $m \in \mathcal{M}_r$. In particular, the query complexity k of the MVC is equal to the number of monomials in the S-decoding polynomial and is at most 2^r for all $m \in \mathcal{M}_r$. A number $m \in \mathcal{M}_r$ has been called *good* if an S-decoding polynomial with $k < 2^r$ monomials exists when m is used to construct MVC. For example, the three-query LDC of [7] was constructed with the good number $m = 7 \times 73$. Itoh and Suzuki [9] showed that one can reduce the query complexity of MVCs via a composition theorem. In particular, by using the good numbers 511 and 2047, they were able to obtain $9 \cdot 2^{r-4}$-query LDC of length N_r for all $r > 5$. Chee *et al.* [10] showed that if there exist primes t, p_1, p_2 such that $m = 2^t - 1 = p_1 p_2$, then m must be good. They determined 50 new good numbers of the above form and then significantly reduced the query complexity of MVCs.

Since [7, 9, 10], the work of finding good numbers has become interesting. However, the study of [7, 9, 10] was limited to good numbers of the form $m = p_1p_2 \in \mathcal{M}_2$. When $\max\{\alpha_1, \alpha_2\} > 1$, it is not known how to decide a number of the form $m = p_1^{\alpha_1}p_2^{\alpha_2} \in \mathcal{M}_2$ is good except using the very expensive computer search. In this paper, we shall provide two methods for obtaining new good numbers in $\mathcal{M}_2$:

- If $m_1 = p_1^{\alpha_1}p_2^{\alpha_2} \in \mathcal{M}_2$ is good and $m_2 = p_1^{\beta_1}p_2^{\beta_2} \in \mathcal{M}_2$ is a multiple of m_1, then m_2 must be good as well.
- If $m_2 = p_1^{\beta_1}p_2^{\beta_2} \in \mathcal{M}_2$ is good, and there is an S-decoding polynomial of the form $P(X) = X^u + aX^v + b$ for m_2 such that $\gcd(u, v, m_2) = p_1^{\omega_1}p_2^{\omega_2}$, then $m_1 = m_2/(p_1^{\omega_1}p_2^{\omega_2})$ must be good as well.

2. PRELIMINARIES

We denote by $\mathbb{Z}$ and $\mathbb{Z}^+$ the set of integers and positive integers, respectively. For any $n \in \mathbb{Z}^+$, we denote $[n] = \{1, 2, \ldots, n\}$. For any $m \in \mathbb{Z}^+$, we denote by $\mathbb{Z}_m$ the set of integers modulo m and denote by $\mathbb{Z}_m^*$ the multiplicative group of integers modulo m. When m is odd, we have that $2 \in \mathbb{Z}_m^*$ and denote by $\mathrm{ord}_m(2)$ the multiplicative order of 2 in $\mathbb{Z}_m^*$. For a prime power q, we denote by $\mathbb{F}_q$ the finite field of q elements and denote by $\mathbb{F}_q^*$ the multiplicative group of $\mathbb{F}_q$. For any $z \in \mathbb{F}_q^*$, we denote by $\mathrm{ord}_q(z)$ the multiplicative order of z. For any two vectors $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$, we denote by $d_H(x, y) = \{i : i \in [n], x_i \neq y_i\}$ the *Hamming distance* between x and y. For any $x, y \in \mathbb{Z}_m^h$, we denote by $\langle x, y\rangle_m = \sum_{i=1}^n x_iy_i \bmod m$ the dot product of x and y. If the components of a vector y are labeled by a set V, then for every $v \in V$ we denote by $y[v]$ the vth component of y.

Definition 2.1. ***(locally decodable code)*** *Let $k, n, N \in \mathbb{Z}^+$ and let $0 \leq \delta, \epsilon \leq 1$. A code $C : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^N$ is said to be (k, δ, ε)-locally decodable if there exist randomized decoding algorithms $D_1, D_2, \ldots, D_n$ such that:*

- *For any $x \in \mathbb{F}_q^n$, any $y \in \mathbb{F}_q^N$ such that $d_H(C(x), y) \leq \delta N$ and any $i \in [n]$, $\Pr[D_i(y) = x_i] \geq 1 - \epsilon$.*
- *The algorithm D_i makes at most k queries to y.*

The numbers k and N are called the *query complexity* and the *length* of C, respectively. They are usually considered as functions of n, the *message length*, and measure the efficiency of C. Ideally, we would like k and N to be as small as possible.

Efremenko [7] proposed a construction of LDCs, which is based on two fundamental building blocks: *S-matching family* and *S-decoding polynomial*.

Definition 2.2. ***(S-matching family)*** *Let $m, h, n \in \mathbb{Z}^+$ and let $S \subseteq \mathbb{Z}_m \setminus \{0\}$. A set $\mathcal{U} = \{u_i\}_{i=1}^n \subseteq \mathbb{Z}_m^h$ is said to be an S-matching family if*

- *$\langle u_i, u_i\rangle_m = 0$ for every $i \in [n]$,*
- *$\langle u_i, u_j\rangle_m \in S$ for all $i, j \in [n]$ such that $i \neq j$.*

Encoding: This algorithm encodes any message $x = (x_1, \ldots, x_n) \in \mathbb{F}_{2^t}^n$ as a codeword $C(x) \in \mathbb{F}_{2^t}^{m^h}$ such that:

- the m^h components of $C(x)$ are labeled by the m^h elements of $\mathbb{Z}_m^h$ respectively; and
- for every $v \in \mathbb{Z}_m^h$, the vth component is computed as $C(x)[v] = \sum_{j=1}^n x_j \cdot \gamma^{\langle u_j, v\rangle_m}$.

Decoding: This algorithm takes a word $y \in \mathbb{F}_{2^t}^{m^h}$ and an integer $i \in [n]$ as input. It recovers x_i as follows:

- choose a vector $v \in \mathbb{Z}_m^h$ uniformly and at random.
- output $\gamma^{-\langle u_i, v\rangle_m} \cdot (a_0 \cdot y[v] + \sum_{\ell=1}^{k-1} a_\ell \cdot y[v + b_\ell u_i])$.

FIGURE 1. Efremenko's construction.

Definition 2.3. *(**S-decoding polynomial**) Let $m \in \mathbb{Z}^+$ be odd. Let $t = ord_m(2)$ and let $\gamma \in \mathbb{F}_{2^t}^*$ be a primitive mth root of unity. A polynomial $P(X) \in \mathbb{F}_{2^t}[X]$ is said to be an S-decoding polynomial if*

- *$P(\gamma^s) = 0$ for every $s \in S$,*
- *$P(\gamma^0) = 1$.*

Given an S-matching family $\mathcal{U} = \{u_i\}_{i=1}^n \subseteq \mathbb{Z}_m^h$ and an S-decoding polynomial $P(X) = a_0 + a_1X^{b_1} + \cdots + a_{k-1}X^{b_{k-1}} \in \mathbb{F}_{2^t}[X]$, Efremenko's LDC can be described in **Figure 1**.

Efremenko's construction gives a linear $(k, \delta, k\delta)$-LDC that encodes messages of length n to codewords of length $N = m^h$. When N is fixed, the larger the n is, the more efficient the C is. Efremenko [7] and several later works [9, 10] choose S as the canonical set in $\mathbb{Z}_m$. For any $m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r} \in \mathcal{M}_r$, the *canonical set* in $\mathbb{Z}_m$ is defined as

$$S_m = \left\{s_\sigma : \sigma \in \{0,1\}^r \setminus \{0^r\}, s_\sigma \equiv \sigma_i(\mathrm{mod} \sim p_i^{\alpha_i}), \forall i \in [r]\right\}.$$

For example, $S_{15} = \{1, 6, 10\}$. Efremenko [7] observed that Grolmusz's set system [11] gives a direct construction of S_m-matching families.

Lemma 2.1. ***([7, 11])*** *For any $m \in \mathcal{M}_r(r \geq 2)$ and integer $h > 0$, there is an S_m-matching family $\mathcal{U} = \{u_i\}_{i=1}^n \subseteq \mathbb{Z}_m^h$ of size $n \geq \exp(c(\log h)^r/(\log\log h)^{r-1})$, where c is a constant that only depends on m.*

In particular, the n takes the form of ℓ^ℓ for an integer $\ell > 0$ and h is determined by both m, ℓ, and the weak representation of the function OR_ℓ [11]. Efremenko [7] also observed that the polynomial $P(X) = \prod_{s\in S_m}(X-\gamma^s)/(1-\gamma^s)$ is an S_m-decoding polynomial with $k \le 2^r$ monomials.

LEMMA 2.2. *([7]) For any $m \in \mathcal{M}_r (r \ge 2)$, there is an S_m-decoding polynomial with at most 2^r monomials.*

Lemmas 2.1 and 2.2 yield LDCs of subexponential length.

THEOREM 2.1. *([7]) For every integer $r \ge 2$, there is a $(k, \delta, k\delta)$-LDC of query complexity $k \le 2^r$ and length N_r.*

For every integer $r \ge 2$, Theorem 2.1 gives an infinite family of LDCs, each based on a number $m \in \mathcal{M}_r$. Different $m \in \mathcal{M}_r$ may give LDCs of different query complexity. For example, $m = 7 \times 73$ gives a code of query complexity 3 [7], while $m = 3 \times 5$ is only able to give a code of query complexity 4 [9]. A number of the form $m = p_1p_2$ has been called *good* in [9, 10] if it is able to result in an LDC of query complexity < 4. By using the good numbers 511 and 2047, Itoh and Suzuki [9] concluded that for any $r > 5$, the query complexity 2^r of the LDCs in Theorem 2.1 can be reduced to $9 \cdot 2^{r-4}$. On the other hand, for $r = 2, 3, 4$ and 5, the best decoding algorithms to date for the LDCs in Theorem 2.1 have query complexity 3, 8, 9 and 24, respectively. Chee *et al.* [10] showed that Mersenne numbers of the form p_1p_2 are good. With infinitely many such good numbers, Chee *et al.* [10] can further reduce the query complexity to $3^{r/2}$.

3. GOOD NUMBERS OF THE FORM $p_1^{\alpha_1}p_2^{\alpha_2}$

Let $m = p_1^{\alpha_1}p_2^{\alpha_2} \in \mathcal{M}_2$. Let $t = \mathrm{ord}_m(2)$ and let $\gamma \in \mathbb{F}_{2^t}^*$ be a primitive mth root of unity. Lemma 2.2 shows that there is an S_m-decoding polynomial $P(X)$ with $k \le 4$ monomials. In this section, we will establish several sufficient and necessary conditions for a number m to be good.

LEMMA 3.1. *Let $m = p_1^{\alpha_1}p_2^{\alpha_2} \in \mathcal{M}_2$. Then any S_m-decoding polynomial has ≥ 3 monomials.*

Proof. If $P(X) = aX^u \in \mathbb{F}_{2^t}[X]$ is an S_m-decoding polynomial, then $a = P(1) = 1$ and $a = \gamma^{-u}P(\gamma) = 0$, which give a contradiction. If $P(X) = aX^u+bX^v \in \mathbb{F}_{2^t}[X]$ is an S_m-decoding polynomial with 2 monomials, then $ab \neq 0$ and

$$a\gamma^{us_{01}} + b\gamma^{vs_{01}} = P(\gamma^{s_{01}}) = 0, \tag{1}$$

$$a\gamma^{us_{10}} + b\gamma^{vs_{10}} = P(\gamma^{s_{10}}) = 0, \tag{2}$$

$$a + b = P(1) \quad = 1. \tag{3}$$

Equations (1) and (2) imply that $b/a = \gamma^{(u-v)s_{01}} = \gamma^{(u-v)s_{10}}$. As $\mathrm{ord}_{2^t}(\gamma) = m$, we must have that

$$(u-v)(s_{01} - s_{10}) \equiv 0 \sim (\mathrm{mod} \sim m). \tag{4}$$

Note that $\gcd(s_{01} - s_{10}, m) = 1$. Equation (4) implies $u \equiv v \sim (\mathrm{mod} \sim m)$. It follows that $b/a = \gamma^{(u-v)s_{01}} = 1$ and thus $a + b = 0$, which contradicts to (3). ■

Let $\mathbb{M}_2$ be the set of good numbers in $\mathcal{M}_2$. The following lemmas characterize $\mathbb{M}_2$.

LEMMA 3.2. *Let $m = p_1^{\alpha_1}p_2^{\alpha_2} \in \mathcal{M}_2$. Then $m \in \mathbb{M}_2$ if and only if there is a polynomial $Q(X) = X^u + aX^v + b \in \mathbb{F}_{2^t}[X]$ that satisfies the following properties*

① $ab \neq 0$,
② $|\{(u \mathrm{mod} \sim m), (v \mathrm{mod} \sim m), 0\}| = 3$, *and*
③ $Q(\gamma) = Q(\gamma^{s_{01}}) = Q(\gamma^{s_{10}}) = 0$, $Q(1) \neq 0$.

Proof. If $m \in \mathbb{M}_2$, then by Lemma 3.1 there exists an S_m-decoding polynomial

$$P(X) = c_1X^{d_1} + c_2X^{d_2} + c_3X^{d_3} \in \mathbb{F}_{2^t}[X] \tag{5}$$

with exactly three monomials. In particular, we must have

④ $c_1c_2c_3 \neq 0$,
⑤ $|\{(d_1 \mathrm{mod} \sim m), (d_2 \sim \mathrm{mod} \sim m), (d_3 \sim \mathrm{mod} \sim m)\}| = 3$, and
⑥ $P(\gamma^{s_{01}}) = P(\gamma^{s_{10}}) = P(\gamma) = 0, P(1) = 1$.

While ④ and ⑥ are clear from the definition, we show that ⑤ is also true. Assume for contradiction that $d_1 \equiv d_2 (\mathrm{mod} \sim m)$. Then $(\gamma^s)^{d_1} = (\gamma^s)^{d_2}$ for all $s \in \{s_{01}, s_{10}, 1\}$ and thus

$$(c_1 + c_2)\gamma^{s_{01}d_1} + c_3\gamma^{s_{01}d_3} = P(\gamma^{s_{01}}) = 0, \tag{6}$$

$$(c_1 + c_2)\gamma^{s_{10}d_1} + c_3\gamma^{s_{10}d_3} = P(\gamma^{s_{10}}) = 0, \tag{7}$$

$$c_1 + c_2 + c_3 = P(1) \quad = 1. \tag{8}$$

Due to (6) and (7), we have that $\gamma^{s_{01}(d_3-d_1)} = \gamma^{s_{10}(d_3-d_1)}$ and thus $d_1 \equiv d_3 (\mathrm{mod} \sim m)$. Consequently, (6) implies that $c_1 + c_2 + c_3 = 0$, which contradicts to (8).

W.l.o.g., we suppose that $d_1 > d_2 > d_3$. Let $u = d_1 - d_3, v = d_2 - d_3, a = c_2/c_1$ and $b = c_3/c_1$. Then

$$Q(X) := X^u + aX^v + b = \frac{P(X)}{c_1X^{d_3}}. \tag{9}$$

The properties ①, ② and ③ trivially follow from ④, ⑤ and ⑥, respectively.

Conversely, suppose that $Q(X) = X^u + aX^v + b$ is a polynomial that satisfies the properties ①, ② and ③. Then $P(X) = Q(X)/Q(1)$ will be an S_m-decoding polynomial with exactly three monomials. Therefore, $m \in \mathbb{M}_2$. ■

LEMMA 3.3. *Let $m = p_1^{\alpha_1}p_2^{\alpha_2} \in \mathcal{M}_2$. Then $m \in \mathbb{M}_2$ if and only if there exist $u, v \in E := \{e : p_1^{\alpha_1} \nmid e, p_2^{\alpha_2} \nmid e, e \in \mathbb{Z}\}$ such that*

$u \not\equiv v(\text{mod} \sim m)$ *and* $\det(A) = 0$, *where*

$$A = \begin{pmatrix} \gamma^{s_{01}u} & \gamma^{s_{01}v} & 1 \\ \gamma^{s_{10}u} & \gamma^{s_{10}v} & 1 \\ \gamma^{u} & \gamma^{v} & 1 \end{pmatrix}. \tag{10}$$

Proof. If $m \in \mathbb{M}_2$, then there is a polynomial $Q(X) = X^u + aX^v + b \in \mathbb{F}_{2^t}[X]$ such that the ①, ② and ③ in Lemma 3.2 are true. Due to ②, we have that $u \not\equiv v(\text{mod} \sim m)$. On the other hand, ③ is equivalent to

$$A \begin{pmatrix} 1 \\ a \\ b \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \tag{11}$$

$$1 + a + b \neq 0. \tag{12}$$

Equation (11) requires that $\det(A) = 0$. It remains to show that $u, v \in E$. We show that $p_1^{\alpha_1} \nmid u$. The proofs for $p_2^{\alpha_2} \nmid u, p_1^{\alpha_1} \nmid v$ and $p_2^{\alpha_2} \nmid v$ will be similar and omitted. Note that

$$\begin{aligned} 0 = \det(A) &= (\gamma^{s_{01}u} + \gamma^{u})(\gamma^{s_{10}v} + \gamma^{v}) + \\ &(\gamma^{s_{01}v} + \gamma^{v})(\gamma^{s_{10}u} + \gamma^{u}) \\ =&((\gamma^{-s_{10}u} + 1)(\gamma^{-s_{01}v} + 1) + \\ &(\gamma^{-s_{01}u} + 1)(\gamma^{-s_{10}v} + 1))\gamma^{u+v}. \end{aligned} \tag{13}$$

If $p_1^{\alpha_1} | u$, then $s_{10}u \equiv 0 \sim (\text{mod} \sim m)$ and $\gamma^{-s_{10}u} + 1 = 0$. Equation (13) would imply $\gamma^{-s_{01}u} + 1 = 0$ or $\gamma^{-s_{10}v} + 1 = 0$. If $\gamma^{-s_{01}u} + 1 = 0$, then $p_2^{\alpha_2} | u$ and thus $m | u$, which would contradicts to ②. If $\gamma^{-s_{10}v} + 1 = 0$, then $p_1^{\alpha_1} | v$ and thus $0 = Q(\gamma^{s_{10}}) = 1 + a + b$, which contradicts to (12).

Conversely, suppose that $u, v \in E$ are integers such that $u \not\equiv v(\text{mod} \sim m)$ and $\det(A) = 0$. To show that $m \in \mathbb{M}_2$, it suffices to construct an S_m-decoding polynomial $Q(X) = X^u + aX^v + b \in \mathbb{F}_{2^t}[X]$ such that ①, ② and ③ are satisfied. First of all, $\det(A) = 0$ implies that $\text{rank}(A) \leq 2$. If $\text{rank}(A) = 1$, then we must have that $\gamma^{s_{01}u} = \gamma^{s_{10}u}$. It follows that $u \equiv 0(\text{mod} \sim m)$, which contradicts to $u \in E$. As $\text{rank}(A) = 2$, the null space of A will be one-dimensional and spanned by a nonzero vector $c = (c_1, c_2, c_3)^T$. Below we shall see that $c_i \neq 0$ for all $i \in [3]$. If $c_1 = 0$, then

$$\begin{pmatrix} \gamma^{s_{01}v} & 1 \\ \gamma^{s_{10}v} & 1 \\ \gamma^{v} & 1 \end{pmatrix} \begin{pmatrix} c_2 \\ c_3 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \tag{14}$$

Then c_2c_3 must be nonzero and thus $\gamma^{s_{01}v} = \gamma^{s_{10}v}$. The latter equality requires that $v \equiv 0(\text{mod} \sim m)$, which contradicts to the fact $v \in E$. Hence, $c_1 \neq 0$. Similarly, we have $c_2 \neq 0$ and $c_3 \neq 0$. Let $R(X) = c_1X^u + c_2X^v + c_3$. Then $R(\gamma) = R(\gamma^{s_{01}}) = R(\gamma^{s_{10}}) = 0$. Furthermore, we must have $R(1) \neq 0$. Otherwise, $c_3 = c_1 + c_2$ and

$$\begin{pmatrix} \gamma^{s_{01}u} + 1 & \gamma^{s_{01}v} + 1 \\ \gamma^{s_{10}u} + 1 & \gamma^{s_{10}v} + 1 \\ \gamma^{u} + 1 & \gamma^{v} + 1 \end{pmatrix} \begin{pmatrix} c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}. \tag{15}$$

As $c_1c_2 \neq 0$, this is possible only if

$$\frac{\gamma^{s_{01}u} + 1}{\gamma^{s_{01}v} + 1} = \frac{\gamma^{s_{10}u} + 1}{\gamma^{s_{10}v} + 1} = \frac{\gamma^{u} + 1}{\gamma^{v} + 1}. \tag{16}$$

Denote by λ the value of the fractions in (16). Then

$$\begin{aligned} &\frac{\gamma^{s_{10}u}}{\gamma^{s_{10}v}} \cdot \sim \underbrace{\frac{\gamma^{s_{01}u} + 1}{\gamma^{s_{01}v} + 1}}_{\lambda} \sim = \frac{\gamma^{s_{10}u} + \gamma^{u}}{\gamma^{s_{10}v} + \gamma^{v}} \\ &= \frac{\gamma^{s_{10}u} + 1 + \gamma^{u} + 1}{\gamma^{s_{10}v} + 1 + \gamma^{v} + 1} \\ &= \frac{\lambda(\gamma^{s_{10}v} + 1) + \lambda(\gamma^{v} + 1)}{\gamma^{s_{10}v} + 1 + \gamma^{v} + 1} \\ &= \lambda, \end{aligned} \tag{17}$$

where the first equality is based on the fact that $s_{01} + s_{10} \equiv 1(\text{mod} \sim m)$ and the second equality is true because we are working over a finite field of characteristic 2. It follows from (17) that $\gamma^{s_{10}(u-v)} = 1$. Therefore, we must have that $u \equiv v(\text{mod} \sim p_1^{\alpha_1})$. Similarly, we have that $u \equiv v(\text{mod} \sim p_2^{\alpha_2})$. Based on the two congruences, we have that $u \equiv v(\text{mod} \sim m)$, which gives a contradiction. Hence, $R(1) \neq 0$ and $Q(X) := R(X)/c_1$ is a polynomial satisfying ①, ②, and ③. ■

LEMMA 3.4. *Let* $m = p_1^{\alpha_1} p_2^{\alpha_2} \in \mathcal{M}_2$. *Let* $t = ord_m(2)$ *and let* $\gamma \in \mathbb{F}_{2^t}^*$ *be a primitive mth root of unity. Let*

$$\tau(z_1, z_2) = \frac{z_1 + z_2}{z_1z_2 + z_2}.$$

Then $m \in \mathbb{M}_2$ *if and only if* τ *is not injective on* $\mathcal{D} = \{(z_1, z_2) \in (\mathbb{F}_{2^t}^* \setminus \{1\})^2 : ord_{2^t}(z_1) | p_1^{\alpha_1}, ord_{2^t}(z_2) | p_2^{\alpha_2}\}$.

Proof. If $m \in \mathbb{M}_2$, then by Lemma 3.3 there exist $u, v \in E$ such that $u \not\equiv v(\text{mod} \sim m)$ and $\det(A) = 0$, where A is defined by (10). Note that $\det(A) = 0$ requires that

$$\frac{\gamma^{s_{10}u} + \gamma^{s_{01}u}}{\gamma^{u} + \gamma^{s_{01}u}} = \frac{\gamma^{s_{10}v} + \gamma^{s_{01}v}}{\gamma^{v} + \gamma^{s_{01}v}}.$$

Clearly, $(\gamma^{s_{10}u}, \gamma^{s_{01}u})$ and $(\gamma^{s_{10}v}, \gamma^{s_{01}v})$ are two distinct elements of $\mathcal{D}$ and $\tau(\gamma^{s_{10}u}, \gamma^{s_{01}u}) = \tau(\gamma^{s_{10}v}, \gamma^{s_{01}v})$. Hence, τ is not injective on $\mathcal{D}$.

Conversely, suppose that $\tau(z_1, z_2) = \tau(z_1', z_2')$ for two distinct elements $(z_1, z_2), (z_1', z_2') \in \mathcal{D}$. To show that $m \in \mathbb{M}_2$, by

Lemma 3.3 it suffices to find $u, v \in E$ such that $u \not\equiv v(\text{mod} \sim m)$ and $\det(A) = 0$. Suppose that

$$\text{ord}_{2^t}(z_1) = p_1^{i_1}, \text{ord}_{2^t}(z_2) = p_2^{j_1},$$
$$\text{ord}_{2^t}(z_1') = p_1^{i_2}, \text{ord}_{2^t}(z_2') = p_2^{j_2}$$

for $i_1, i_2 \in [\alpha_1]$ and $j_1, j_2 \in [\alpha_2]$. Then there exist integers u_1, u_2, v_1, v_2, where $p_1 \nmid u_1, v_1$ and $p_2 \nmid u_2, v_2$, such that

$$z_1 = (\gamma^{s_{10}p_1^{\alpha_1 - i_1}})^{u_1}, z_2 = (\gamma^{s_{01}p_2^{\alpha_2 - j_1}})^{u_2},$$
$$z_1' = (\gamma^{s_{10}p_1^{\alpha_1 - i_2}})^{v_1}, z_2' = (\gamma^{s_{01}p_2^{\alpha_2 - j_2}})^{v_2}.$$

By Chinese remainder theorem, there exist u, v such that:

$$\begin{cases} u \equiv p_1^{\alpha_1 - i_1} u_1(\text{mod} \sim p_1^{\alpha_1}), \\ u \equiv p_2^{\alpha_2 - j_1} u_2(\text{mod} \sim p_2^{\alpha_2}), \end{cases} \quad \begin{cases} v \equiv p_1^{\alpha_1 - i_2} v_1(\text{mod} \sim p_1^{\alpha_1}), \\ v \equiv p_2^{\alpha_2 - j_2} v_2(\text{mod} \sim p_2^{\alpha_2}). \end{cases}$$

In particular, $u, v \in E$ and $u \not\equiv v(\text{mod} \sim m)$ (o.w., we will have $(z_1, z_2) = (z_1', z_2')$). Furthermore, $z_1 = \gamma^{s_{10}u}, z_2 = \gamma^{s_{01}u}, z_1' = \gamma^{s_{10}v}$ and $z_2' = \gamma^{s_{01}v}$. Since $\tau(z_1, z_2) = \tau(z_1', z_2')$, we must have that $\det(A) = 0$ due to (13). ■

Let $\rho(z_1, z_2) = \tau(z_1, z_2) - 1 = (1 + z_2^{-1})(1 + z_1^{-1})^{-1}$. Then Lemma 3.4 gives the following theorem.

THEOREM 3.1. *Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \in \mathcal{M}_2$. Let $t = ord_m(2)$ and let $\gamma \in \mathbb{F}_{2^t}^*$ be a primitive mth root of unity. Then $m \in \mathbb{M}_2$ if and only if ρ is not injective on $\mathcal{D}$.*

Theorem 3.1 gives a characterization of the good numbers in $\mathcal{M}_2$. We say that $(u, v) \in E^2$ form a *collision* for m if

- $\rho(\gamma^{s_{10}u}, \gamma^{s_{01}u}) = \rho(\gamma^{s_{10}v}, \gamma^{s_{01}v})$, and
- $u \not\equiv v(\text{mod} \sim m)$.

The proof of Lemma 3.4 shows that $m \in \mathbb{M}_2$ if and only if there is a collision $(u, v) \in E^2$ for m.

4. IMPLICATIONS BETWEEN GOOD NUMBERS

In this section, we show the implications between good numbers in $\mathcal{M}_2$, which allows us to construct new good numbers from old.

LEMMA 4.1. *Let $m_1 = p_1^{\alpha_1} p_2^{\alpha_2}, m_2 = p_1^{\beta_1} p_2^{\beta_2} \in \mathcal{M}_2$. Let $t_i = ord_{m_i}(2)$ and let $\gamma_i \in \mathbb{F}_{2^{t_i}}^*$ be a primitive m_ith root of unity for $i = 1, 2$. If $m_1 | m_2$, then there is an integer $\sigma \in \mathbb{Z}_{m_1}^*$ such that $\gamma_1 = \gamma_2^{\sigma m_2/m_1}$.*

Proof. As $m_1 | m_2$ and $m_2 | (2^{t_2} - 1)$, we must have that $t_1 | t_2$. Then $\mathbb{F}_{2^{t_1}}$ is a subfield of $\mathbb{F}_{2^{t_2}}$. Note that $\gamma_1 \in \mathbb{F}_{2^{t_1}} \subseteq \mathbb{F}_{2^{t_2}}$ and $\gamma_2^{m_2/m_1} \in \mathbb{F}_{2^{t_2}}$ are elements of the same finite field and have the same multiplicative order (i.e. m_1). Both $\langle \gamma_1 \rangle$ and $\langle \gamma_2^{m_2/m_1} \rangle$ are subgroups of $\mathbb{F}_{2^{t_2}}^*$ of order m_1. As $\mathbb{F}_{2^{t_2}}^*$ has a unique subgroup of order m_1, it must be the case that $\langle \gamma_1 \rangle = \langle \gamma_2^{m_2/m_1} \rangle$. Hence, there is an integer $\sigma \in \mathbb{Z}_{m_1}^*$ such that $\gamma_1 = \gamma_2^{\sigma m_2/m_1}$. ■

THEOREM 4.1. *Let $m_1 = p_1^{\alpha_1} p_2^{\alpha_2}, m_2 = p_1^{\beta_1} p_2^{\beta_2} \in \mathcal{M}_2$. If $m_1 \in \mathbb{M}_2$ and $m_1 | m_2$, then $m_2 \in \mathbb{M}_2$.*

Proof. For $i \in \{1, 2\}$, let $S_{m_i} = \{s_{01}^i, s_{10}^i, 1\}$, let $t_i = \text{ord}_{m_i}(2)$, and let $\gamma_i \in \mathbb{F}_{2^{t_i}}^*$ be of order m_i. Let $E_1 = \{e : p_1^{\alpha_1} \nmid e, p_2^{\alpha_2} \nmid e, e \in \mathbb{Z}\}$ and $E_2 = \{e : p_1^{\beta_1} \nmid e, p_2^{\beta_2} \nmid e, e \in \mathbb{Z}\}$.

If $m_1 \in \mathbb{M}_2$, then there is a collision $(u_1, v_1) \in E^2$ such that $u_1 \not\equiv v_1(\text{mod} \sim m_1)$ and

$$\frac{\gamma_1^{-s_{01}^1 u_1} + 1}{\gamma_1^{-s_{10}^1 u_1} + 1} = \frac{\gamma_1^{-s_{01}^1 v_1} + 1}{\gamma_1^{-s_{10}^1 v_1} + 1}. \tag{18}$$

As per Lemma 4.1, let $\sigma \in \mathbb{Z}_{m_1}^*$ be an integer such that $\gamma_1 = \gamma_2^{\sigma m_2/m_1}$. Then (18) is

$$\frac{\gamma_2^{-s_{01}^1 u_1 \sigma m_2/m_1} + 1}{\gamma_2^{-s_{10}^1 u_1 \sigma m_2/m_1} + 1} = \frac{\gamma_2^{-s_{01}^1 v_1 \sigma m_2/m_1} + 1}{\gamma_2^{-s_{10}^1 v_1 \sigma m_2/m_1} + 1}. \tag{19}$$

We claim that if there exist integers u_2, v_2 such that

$$\text{(i)} \begin{cases} s_{01}^1 u_1 \sigma m_2/m_1 \equiv s_{01}^2 u_2(\text{mod} \sim m_2), \\ s_{10}^1 u_1 \sigma m_2/m_1 \equiv s_{10}^2 u_2(\text{mod} \sim m_2), \end{cases}$$

$$\text{(ii)} \begin{cases} s_{01}^1 v_1 \sigma m_2/m_1 \equiv s_{01}^2 v_2(\text{mod} \sim m_2), \\ s_{10}^1 v_1 \sigma m_2/m_1 \equiv s_{10}^2 v_2(\text{mod} \sim m_2), \end{cases}$$

then $u_2, v_2 \in E_2$, $u_2 \not\equiv v_2(\text{mod} \sim m_2)$ and

$$\frac{\gamma_2^{-s_{01}^2 u_2} + 1}{\gamma_2^{-s_{10}^2 u_2} + 1} = \frac{\gamma_2^{-s_{01}^2 v_2} + 1}{\gamma_2^{-s_{10}^2 v_2} + 1}, \tag{20}$$

i.e. (u_2, v_2) form a collision for m_2 (and thus $m_2 \in \mathbb{M}_2$). Note that (20) is clear from (i), (ii) and (19). We need to show that $u_2, v_2 \in E_2$ and $u_2 \not\equiv v_2(\text{mod} \sim m_2)$. If $p_1^{\beta_1} | u_2$, then we will have that $m_2 | s_{10}^2 u_2$. The second congruence of (i) would imply that $p_1^{\alpha_1} | u_1 \sigma$, which contradicts to $u_1 \in E_1$ and $\sigma \in \mathbb{Z}_{m_1}^*$. Similarly, we have $p_2^{\beta_2} \nmid u_2, p_1^{\beta_1} \nmid v_2$ and $p_2^{\beta_2} \nmid v_2$. Hence, $u_2, v_2 \in E_2$. If $u_2 \equiv v_2(\text{mod} \sim m_2)$, then the first congruences of (i) and (ii) would imply that $s_{01}^1 \sigma(u_1 - v_1) \equiv 0(\text{mod} \sim m_1)$, which requires that $u_1 \equiv v_1(\text{mod} \sim p_2^{\alpha_2})$. Similarly, the second congruences of (i) and (ii) would imply

$u_1 \equiv v_1 (\text{mod} \sim p_1^{\alpha_1})$. It follows that $u_1 \equiv v_1 (\text{mod} \sim m_1)$, which is a contradiction.

It remains to show the existence of integers u_2 and v_2 that satisfy (i) and (ii). We show that existence of u_2. The existence of v_2 is similar. Due to Chinese remainder theorem, the first congruence of (i) is equivalent to

$$\begin{cases} s_{01}^1 u_1 \sigma m_2/m_1 \equiv s_{01}^2 u_2 (\text{mod} \sim p_1^{\beta_1}), \\ s_{01}^1 u_1 \sigma m_2/m_1 \equiv s_{01}^2 u_2 (\text{mod} \sim p_2^{\beta_2}), \end{cases} \tag{21}$$

Note that the first congruence of (21) is always true. On the other hand, as $s_{01}^2 \equiv 1 (\text{mod} \sim p_2^{\beta_2})$, the first congruence of (i) must be equivalent to

$$u_2 \equiv s_{01}^1 u_1 \sigma m_2/m_1 (\text{mod} \sim p_2^{\beta_2}). \tag{22}$$

Similarly, the second congruence of (i) is equivalent to

$$u_2 \equiv s_{10}^1 u_1 \sigma m_2/m_1 (\text{mod} \sim p_1^{\beta_1}). \tag{23}$$

Therefore, (i) is equivalent to the system formed by (22) and (23). The existence of u_2 is an easy consequence of the Chinese remainder theorem. ■

THEOREM 4.2. *Let $m_2 = p_1^{\beta_1} p_2^{\beta_2} \in \mathcal{M}_2$. Suppose that $m_2 \in \mathbb{M}_2$ and $(u, v) = (p_1^{i_1} p_2^{i_2} \sigma_1, p_1^{j_1} p_2^{j_2} \sigma_2)$ is a collision for m_2, where $\sigma_1, \sigma_2 \in \mathbb{Z}_{m_2}^*$. Let $\omega_1 = \min\{i_1, j_1\}$ and $\omega_2 = \min\{i_2, j_2\}$. Then $m_1 := m_2/(p_1^{\omega_1} p_2^{\omega_2})$ belongs to $\mathbb{M}_2$.*

Proof. For $i = 1, 2$, let $S_{m_i} = \{s_{01}^i, s_{10}^i, 1\}$, let $t_i = \text{ord}_{m_i}(2)$ and let $\gamma_i \in \mathbb{F}_{2^{t_i}}^*$ be of order m_i. Let $E_1 = \{e : p_1^{\beta_1 - \omega_1} \nmid e, p_2^{\beta_2 - \omega_2} \nmid e, e \in \mathbb{Z}\}$ and $E_2 = \{e : p_1^{\beta_1} \nmid e, p_2^{\beta_2} \nmid e, e \in \mathbb{Z}\}$. To show that $m_1 \in \mathbb{M}_2$, it suffices to find two integers $u_1, v_1 \in E_1$ such that $u_1 \not\equiv v_1 (\text{mod} \sim m_1)$ and

$$\frac{\gamma_1^{-s_{01}^1 u_1} + 1}{\gamma_1^{-s_{10}^1 u_1} + 1} = \frac{\gamma_1^{-s_{01}^1 v_1} + 1}{\gamma_1^{-s_{10}^1 v_1} + 1}. \tag{24}$$

As per Lemma 4.1, there is an integer $\sigma \in \mathbb{Z}_{m_2}^*$ such that $\gamma_1 = \gamma_2^{p_1^{\omega_1} p_2^{\omega_2} \sigma}$. Then (24) is

$$\frac{\gamma_2^{-s_{01}^1 u_1 p_1^{\omega_1} p_2^{\omega_2} \sigma} + 1}{\gamma_2^{-s_{10}^1 u_1 p_1^{\omega_1} p_2^{\omega_2} \sigma} + 1} = \frac{\gamma_2^{-s_{01}^1 v_1 p_1^{\omega_1} p_2^{\omega_2} \sigma} + 1}{\gamma_2^{-s_{10}^1 v_1 p_1^{\omega_1} p_2^{\omega_2} \sigma} + 1}. \tag{25}$$

As $(p_1^{i_1} p_2^{i_2} \sigma_1, p_1^{j_1} p_2^{j_2} \sigma_2) \in E_2^2$ is a collision for m_2, we have

$$\frac{\gamma_2^{-s_{01}^2 p_1^{i_1} p_2^{i_2} \sigma_1} + 1}{\gamma_2^{-s_{10}^2 p_1^{i_1} p_2^{i_2} \sigma_1} + 1} = \frac{\gamma_2^{-s_{01}^2 p_1^{j_1} p_2^{j_2} \sigma_2} + 1}{\gamma_2^{-s_{10}^2 p_1^{j_1} p_2^{j_2} \sigma_2} + 1}. \tag{26}$$

We claim that if there exist integers u_1, v_1 such that

$$\text{(i)} \begin{cases} s_{01}^1 u_1 p_1^{\omega_1} p_2^{\omega_2} \sigma \equiv s_{01}^2 p_1^{i_1} p_2^{i_2} \sigma_1 (\text{mod} \sim m_2), \\ s_{10}^1 u_1 p_1^{\omega_1} p_2^{\omega_2} \sigma \equiv s_{10}^2 p_1^{i_1} p_2^{i_2} \sigma_1 (\text{mod} \sim m_2), \end{cases}$$

$$\text{(ii)} \begin{cases} s_{01}^1 v_1 p_1^{\omega_1} p_2^{\omega_2} \sigma \equiv s_{01}^2 p_1^{j_1} p_2^{j_2} \sigma_2 (\text{mod} \sim m_2), \\ s_{10}^1 v_1 p_1^{\omega_1} p_2^{\omega_2} \sigma \equiv s_{10}^2 p_1^{j_1} p_2^{j_2} \sigma_2 (\text{mod} \sim m_2), \end{cases}$$

then $u_1, v_1 \in E_1$, $u_1 \not\equiv v_1 (\text{mod} \sim m_1)$ and (25) holds. Note that (25) is clear from (i), (ii) and (26). If $p_1^{\beta_1 - \omega_1} | u_1$, then the second congruence of (i) would imply that $p_1^{\beta_1} | p_1^{i_1} p_2^{i_2} \sigma_1$, which contradicts to the fact that $p_1^{i_1} p_2^{i_2} \sigma_1 \in E_2$. Similarly, we can show that $p_2^{\beta_2 - \omega_2} \nmid u_1, p_1^{\beta_1 - \omega_1} \nmid v_1$ and $p_2^{\beta_2 - \omega_2} \nmid v_1$. Therefore, $u_1, v_1 \in E_1$. If $u_1 \equiv v_1 (\text{mod} \sim m_1)$, then the first congruences of (i) and (ii) would imply that $s_{01}^2 (p_1^{i_1} p_2^{i_2} \sigma_1 - p_1^{j_1} p_2^{j_2} \sigma_2) \equiv 0 (\text{mod} \sim m_2)$, which requires that $p_1^{i_1} p_2^{i_2} \sigma_1 \equiv p_1^{j_1} p_2^{j_2} \sigma_2 (\text{mod} \sim p_2^{\beta_2})$. Similarly, the second congruences of (i) and (ii) require that $p_1^{i_1} p_2^{i_2} \sigma_1 \equiv p_1^{j_1} p_2^{j_2} \sigma_2 (\text{mod} \sim p_1^{\beta_1})$. It follows that $p_1^{i_1} p_2^{i_2} \sigma_1 \equiv p_1^{j_1} p_2^{j_2} \sigma_2 (\text{mod} \sim m_2)$, which is a contradiction.

It remains to show the existence of u_1 and v_1 that satisfy (i) and (ii). We show the existence of u_1. The existence of v_1 is similar and omitted. As $\omega_1 \le i_1 \le \beta_1$ and $\omega_2 \le i_2 \le \beta_2$, the first congruence in (i) is equivalent to

$$\begin{cases} s_{01}^1 u_1 \sigma \equiv s_{01}^2 p_1^{i_1 - \omega_1} p_2^{i_2 - \omega_2} \sigma_1 (\text{mod} \sim p_1^{\beta_1 - \omega_1}), \\ s_{01}^1 u_1 \sigma \equiv s_{01}^2 p_1^{i_1 - \omega_1} p_2^{i_2 - w_2} \sigma_1 (\text{mod} \sim p_2^{\beta_2 - \omega_2}). \end{cases} \tag{27}$$

Note that the first congruence of (27) is always true. On the other hand, as $p_2 \nmid s_{01}^1 \sigma$, there is an integer t_{01}^1 such that $s_{01}^1 \sigma t_{01}^1 \equiv 1 (\text{mod} \sim p_2^{\beta_2 - \omega_2})$. Therefore, the first congruence of (i) will be equivalent to

$$u_1 \equiv s_{01}^2 t_{01}^1 p_1^{i_1 - \omega_1} p_2^{i_2 - \omega_2} \sigma_1 (\text{mod} \sim p_2^{\beta_2 - \omega_2}). \tag{28}$$

Similarly, we can show that the second congruence of (i) is equivalent to

$$u_1 \equiv s_{10}^2 t_{10}^1 p_1^{i_1 - \omega_1} p_2^{i_2 - \omega_2} \sigma_1 (\text{mod} \sim p_1^{\beta_1 - \omega_1}), \tag{29}$$

where t_{10}^1 is an integer such that $s_{10}^1 \sigma t_{10}^1 \equiv 1 (\text{mod} \sim p_1^{\beta_1 - \omega_1})$. The existence of u_1 is an easy consequence of the Chinese remainder theorem on (28) and (29). ■

EXAMPLE 1. Let $m_2 = 7^2 \times 151$. Then $S_{m_2} = \{s_{01} = 1813, s_{10} = 5587, s_{11} = 1\}$. Let $t_2 = \text{ord}_{m_2}(2)$ and let $\gamma_2 \in \mathbb{F}_{2^{t_2}}^*$ be a primitive m_2th root of unity. Then $(238, 455)$ is a collision for m_2. Clearly, $\omega_1 = 1$ and $\omega_2 = 0$. Then $m_1 = m_2/7 = 1057$ must be a good number, which is $< m_2$.

5. CONCLUSION

In this paper, we characterized the good numbers in $\mathcal{M}_2$ and showed two implications between good numbers in $\mathcal{M}_2$. In particular, the second implication requires an additional condition. It is an interesting problem to remove the condition.

DATA AVAILABILITY STATEMENT

No new data were generated or analysed in support of this research.

ACKNOWLEDGEMENTS

The authors would like to thank the anonymous reviewers for their helpful suggestions.

FUNDING

Natural Science Foundation of Shanghai (21ZR1443000); Singapore Ministry of Education (RG12/19).

REFERENCES

[1] Katz, J. and Trevisan, L. (2000) On the Efficiency of Local Decoding Procedures for Error-Correcting Codes. In Yao, F., Luks, E.M. (eds) *Proc. 32nd Annual ACM SIGACT Symposium on Theory of Computing, STOC 2000*, Portland, OR, USA, May 21–23, 2000, pp. 80–86. ACM, New York.

[2] Gasarch, W. (2004) A survey on private information retrieval. *Bulletin of the EATCS*, 82, 72–107.

[3] Trevisan, L. (2004) Some Applications of Coding Theory in Computational Complexity. Electronic Colloquium on Computational Complexity, 11, No. 043.

[4] Goldreich, O., Karloff, H.J., Schulman, L.J. and Trevisan, L. (2006) Lower bounds for linear locally decodable codes and private information retrieval. *Comput. Complex.*, 15, 263–296.

[5] Woodruff, D.P. (2007) New Lower Bounds for General Locally Decodable Codes. Electronic Colloquium on Computational Complexity, 14, No. 006.

[6] Yekhanin, S. (2008) Towards 3-query locally decodable codes of subexponential length. *J. ACM*, 55, 1:1–1:16.

[7] Efremenko, K. (2012) 3-query locally decodable codes of subexponential length. *SIAM J. Comput.*, 41, 1694–1703.

[8] Dvir, Z., Gopalan, P. and Yekhanin, S. (2011) Matching vector codes. *SIAM J. Comput.*, 40, 1154–1178.

[9] Itoh, T. and Suzuki, Y. (2010) Improved constructions for query-efficient locally decodable codes of subexponential length. *IEICE Trans. Inf. Syst.*, E93–D, 263–270.

[10] Chee, Y.M., Feng, T., Ling, S., Wang, H. and Zhang, L.F. (2013) Query-efficient locally decodable codes of subexponential length. *Comput. Complex.*, 22, 159–189.

[11] Grolmusz, V. (2000) Superpolynomial size set-systems with restricted intersections mod 6 and explicit Ramsey graphs. *Combinatorica*, 20, 71–86.