Multicast Network Coding and Field Sizes

Qifu (Tyler) Sun†, Xunrui Yin†, Zongpeng Li‡, and Keping Long†
†Institute of Advanced Networking Technology and New Service,
University of Science and Technology Beijing, Beijing, P. R. China
‡ Department of Computer Science, University of Calgary, Calgary, Canada
Email: {qfsun, longkeping}@ustb.edu.cn, {xunyin, zongpeng}@ucalgary.ca

Abstract—In an acyclic multicast network, it is well known that a linear network coding solution over GF(q) exists when q is sufficiently large. In particular, for each prime power q no smaller than the number of receivers, a linear solution over GF(q) can be efficiently constructed. In this work, we reveal that a linear solution over a given finite field does not necessarily imply the existence of a linear solution over all larger finite fields. Specifically, we prove by construction that: (i) For every source dimension no smaller than 3, there is a multicast network linearly solvable over GF(7) but not over GF(8), and there is another multicast network linearly solvable over GF(16) but not over GF(17); (ii) There is a multicast network linearly solvable over GF(5) but not over such GF(q) that q > 5 is a Mersenne prime plus 1, which can be extremely large.

Index Terms—Linear network coding, multicast network, field size, Mersenne prime.

I. INTRODUCTION

Consider a multicast network, which is a finite directed acyclic multigraph with a unique source node s and a set T of receivers. Every edge in the network represents a noiseless transmission channel of unit capacity. The source generates ω data symbols belonging to a fixed symbol alphabet and will transmit them to all receivers via the network. The maximum flow, which is equal to the number of edge-disjoint paths, from s to every receiver is assumed to be no smaller than ω. The network is said to be solvable if all receivers can recover all ω source symbols based on their respective received data symbols. When the network has only one receiver, it is solvable by network routing. When |T| > 1, the paradigm of network routing does not guarantee the network to be solvable. The seminal paper [2] introduced the concept of network coding (NC) and proved that the network has a NC solution over some infinitely large symbol alphabet. It was further shown in [1] that linear NC suffices to yield a solution when the symbol alphabet is algebraically modeled as a sufficiently large finite field, and every intermediate node transmits a linear combination of its received data symbols over the symbol field. Since then, there have been extensive studies on the field size requirement of a linear solution for a multicast network.

From an algebraic approach, reference [2] first showed that a multicast network has a linear solution over GF(q) as long as the prime power q is larger than ω times the number |T| of receivers. The requirement of q for the existence of a linear solution over GF(q) is further relaxed by [3] to be larger than |T|, and such a solution can be efficiently constructed by the algorithm proposed in [4]. Meanwhile, the efficient algorithm in [5] is able to construct a linear solution over GF(q) when q is no smaller than |T|, and hence this condition on q is slightly relaxed compared with the ones in [3] and [4]. This efficient algorithm requires to initially identify, for each receiver in T, ω edge-disjoint paths starting from the source and ending at it. Denote by η the maximum number of paths among the ω|T| that contain a common edge. The parameter η is always no larger than |T|. By a more elaborate argument, the algorithm in [5] is refined in [6] such that it can construct a linear solution over GF(q) as long as q is no smaller than η.

Denote by qmin the minimum field size for the existence of a linear solution over GF(qmin), and by qmax the maximum field size for the non-existence of a linear solution over GF(qmax) (if the network is linearly solvable over every finite field, then qmax is not well defined and we set it to 1 as a convention.) The algorithm in [5] implies that |T| is an upper bound on qmax. For the special case that the source dimension ω is equal to 2, the upper bound on qmax is reduced to O(√|T|) in [7]. In both cases, the upper bounds additionally guarantee the existence of a linear solution over every GF(q) with q larger than the bounds. On the other hand, references [8] and [9] independently constructed a class of multicast networks with qmin lower bounded by Θ(√|T|). On any network in this class, a linear solution exists over every GF(q) with q no smaller than qmin, that is, qmax < qmin. These results indicate that in many cases, an acyclic multicast network that is linearly solvable over a given finite field GF(q) is also linearly solvable over every larger finite field.

To the best of our knowledge, there is no explicit proof or disproof of the above claim for a general multicast network and for the case q < |T|; furthermore, all known multicast networks studied in the network coding literature satisfy qmax < qmin. Although it has been shown in [10] that the (4,2)-combination network depicted in Fig. 1 has a nonlinear solution over a ternary symbol alphabet but has neither a linear nor a nonlinear solution over any symbol alphabet of size 6, it does not shed light on disproving the claim (**) because this combination network has a linear solution over every GF(q) with q ≥ 3 (See, for example, [11].) Moreover, in the case ω = 2, as revealed in [9] and [7], there exists a linear solution over GF(q) if and only if there exists a (q − 1)-vertex coloring in an appropriately defined associated graph. Since a q-vertex coloring in a graph always guarantees a q'-vertex coloring with...
$q' > q$ in the same graph, a multicast network with $\omega = 2$ is linearly solvable over every GF($q'$) with $q' \geq q_{\min}$. This evidence seemed to add more support for the correctness of the claim ($\ast$) for an arbitrary multicast network.

In the present paper, we shall show by constructive proofs that the claim ($\ast$) is not always true. In particular,

- we show that there is a multicast network that is linearly solvable over GF($q_{\min}$) but not over GF($q_{\max}^*$) for each of: (i) $q_{\min} = 5$, $q_{\max}^* = 8$; (ii) $q_{\min} = 7$, $q_{\max}^* = 8$; (iii) $q_{\min} = 16$, $q_{\max}^* = 17$;
- we show that for any positive integer $d$ with less than 17,425,170 (base-10) digits, there is a multicast network with $q_{\min} = 5$ whereas $q_{\max}^* > d$.

The insight of our results is that not only the field size but also the orders of the proper multiplicative subgroups in the symbol field affect the linear solvability over the finite field. As we shall see, if a finite field does not contain a large enough proper multiplicative subgroup, or the complement of a large multiplicative subgroup in the finite field is not large enough, it is possible to construct a multicast network that is not linearly solvable over this finite field but linearly solvable over a smaller finite field. In comparison, the characteristic of the symbol field does not appear as important in designing examples here as in the ones in [12] which show the non-existence of a linear solution for a general multi-source multicast network. The classical solvable network that is not linearly solvable, proposed in [12], makes use of two types of subnetworks: one is linearly solvable only over a field with even characteristic whereas the other is linearly solvable only over a field with odd characteristic. Consequently, the proposed network as a whole is not linearly solvable over any field, even or odd. Our results bring about a new facet on the connection between the symbol field structures and network coding solvability problems.

The remainder of this paper is organized as follows. Section II presents the fundamental results that there exist multicast networks such that $q_{\min} < q_{\max}^*$. Section III discusses how large the gap $q_{\max}^* - q_{\min}$ can be. Section IV concludes the paper and lists some interesting problems along this new research thread in network coding theory. Due to space limit, all detailed proofs of lemmas in this paper are omitted and they can be found in the technical report [13].

II. FUNDAMENTAL RESULTS

Conventions. A multicast network is a finite directed acyclic multigraph with a unique source node $s$ and a set $T$ of receivers. On a multicast network, for every node $v$, denote by $In(v)$ and $Out(v)$, respectively, the set of its incoming and outgoing edges. Without loss of generality (WLOG), assume that $|Out(s)| = \omega$ (otherwise a new source can be created, connected to the old source with $\omega$ edges). For an arbitrary set $N$ of non-source nodes, denote by $maxflow(N)$ the maximum number of edge-disjoint paths starting from $s$ and ending at nodes in $N$. Each node $t$ in the set $T$ of receivers has $maxflow(t) = \omega$. A linear network code (LNC) over GF($q$) is an assignment of a coding coefficient $k_{d,e} \in$ GF($q$) to every pair $(d,e)$ of edges such that $k_{d,e} = 0$ when $(d,e)$ is not an adjacent pair, that is, when there is not a node $v$ such that $d \in In(v)$ and $e \in Out(v)$. The LNC uniquely determines a coding vector $f_e$, which is an $\omega$-dim column vector, for each edge $e$ in the network such that:

- $\{f_e, e \in Out(s)\}$ forms the natural basis of GF($q$)$^\omega$.
- $f_e = \sum_{d \in In(v)} k_{d,e} f_d$ when $e \in Out(v)$ for some $v \neq s$.

WLOG, we assume throughout this paper that

- all LNCs on a given multicast network have coding coefficients $k_{d,e} = 1$ for all those adjacent pairs $(d,e)$ where $d$ is the unique incoming edge to some node.

A multicast network is said to be linearly solvable over GF($q$) if there is an LNC over GF($q$) such that for each receiver $t \in T$, the $\omega \times |In(t)|$ matrix $[f_e]_{e \in In(t)}$ over GF($q$) is full rank. Such an LNC is called a linear solution over GF($q$) for the multicast network. Denote by $q_{\min}$ the minimum field size for the existence of a linear solution over GF($q_{\min}$), and by $q_{\max}^*$ the maximum field size for the nonexistence of a linear solution over GF($q_{\max}^*$). Specific to a finite field GF($q$), let GF($q^k$) represent the multiplicative group of nonzero elements in GF($q$).

When $q \geq |T|$, the efficient algorithm in [5] can be adopted to construct a linear solution over GF($q$). In the case $\omega = 2$, it has been shown in [9], [7] that every linear solution over GF($q$) can induce a $(q-1)$-vertex coloring in an appropriately associated graph of the multicast network and vice versa. Since every $(q-1)$-vertex coloring in a graph can also be regarded as a $(q'-1)$-vertex coloring for $q' > q$, it in turn induces a linear solution over GF($q'$) when $q'$ is a prime power. Thus, every linear solution over a finite field can induce a linear solution over a larger finite field. All these are tempting facts for one to conjecture that when $\omega > 2$ and $q < |T|$, a linear solution over a finite field might also imply the existence of a linear solution over a larger field. The central theme of the present paper is to refute this conjecture in several aspects.

Theorem 1. A multicast network with $\omega \geq 3$ that is linearly solvable over a finite field is not necessarily linearly solvable over all larger finite fields.
Proof: When \( \omega = 3 \), this theorem is a direct consequence of the lemma below. Assume \( \omega > 3 \). Expand the network \( \mathcal{N} \) depicted in Fig. 2(a) to a new multicast network \( \mathcal{N}' \) as follows. Create \( \omega - 3 \) new nodes each of which has an incoming edge emanating from the source and an outgoing edge entering every receiver. In \( \mathcal{N}' \), every receiver has the maximum flow from the source equal to \( \omega \). Consider an LNC over a given \( \mathbb{GF}(q) \). By the topology of \( \mathcal{N}' \), the coding vector for every edge that is originally in \( \mathcal{N} \) is a linear combination of the coding vectors for those edges in \( \text{Out}(s) \) that are also in \( \mathcal{N} \). Since the network \( \mathcal{N}' \) is linearly solvable over \( \mathbb{GF}(q) \) with every \( q \geq 7 \) except for \( q = 8 \) by the lemma below, so is the network \( \mathcal{N}' \).

Lemma 2. Consider the multicast network depicted in Fig. 2(a). Denote by \( e_i, 1 \leq i \leq 9 \) the unique incoming edge to node \( n_i \). For every set \( N \) of 3 grey nodes with \( \text{maxflow}(N) = 3 \), there is a receiver connected from it. This network is linearly solvable over every finite field \( \mathbb{GF}(q) \) with \( q \geq q_{\min} = 7 \) except for \( q = q_{\max}^* = 8 \).

In the network in Fig. 2(a), observe that every receiver is connected with three nodes \( n_1, n_2, n_3 \) where either \([i/3], [j/3], [k/3]\) are distinct (such as \( \{n_1, n_4, n_5\} \)) or two among \([i/3], [j/3], [k/3]\) are same (such as \( \{n_1, n_2, n_4\} \)). One can then check an LNC over \( \mathbb{GF}(7) \) with

\[
\begin{bmatrix}
1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\
1 & 2 & 4 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 0 & 1 & 2 & 4 & 1 & 2 \\
4 & 1 & 2 & 4 & 1 & 2 & 4 & 1
\end{bmatrix}
\]

qualifies to be a linear solution for the network. Note that all nonzero entries in this matrix belong to a proper subgroup of order 3 in the multiplicative group \( \mathbb{GF}(7)^\times \). The key reason that results in the network not linearly solvable over \( \mathbb{GF}(8) \) is that there is not a proper subgroup of order no smaller than 3 in the multiplicative group \( \mathbb{GF}(8)^\times \). In general, it can be shown that the network in Fig. 2(a) is linearly solvable over a finite field \( \mathbb{GF}(q) \) if and only if there exist \( \alpha_i, \beta_i, \delta_i \in \mathbb{GF}(q)^\times, 1 \leq i \leq 3 \) subject to

\[
\alpha_i \neq \alpha_j, \beta_i \neq \beta_j, \delta_i \neq \delta_j, \quad \forall \ 1 \leq i < j \leq 3,
\]

\[
\{\delta_1, \delta_2, \delta_3\} \subseteq \mathbb{GF}(q)^\times \{\alpha_i \beta_j : 1 \leq i, j \leq 3\}.
\]

A detailed technical proof for Lemma 2 can be found in [13].

On a solvable multi-source multicast network, it is well-known that linear network coding (with linearity in terms of a more general algebraic structure) is not sufficient to yield a solution. The classical example in [12] to show this consists of two subnetworks, one is only linearly solvable over a field with even characteristic, whereas the other is only linearly solvable over a field with odd characteristic. More generally, a procedure is introduced in [14] to construct a (matroidal) multi-source multicast network based on a matroid such that the constructed network is linearly solvable over \( \mathbb{GF}(q) \) if and only if the matroid is representable over \( \mathbb{GF}(q) \). This connection is powerful for designing a number of non-linearly solvable networks from a variety of interesting matroid structures (See the Appendix in [15] for example,) and the network in [12] is an instance under this construction. However, the examples of (single-source) multicast networks presented in this paper cannot be established by the procedure introduced in [14]. Moreover, as a result of Lemma 2 and the next lemma, the role of the characteristic of a finite field in the examples designed in the present paper is not as important as in the example in [12].

Lemma 3. Consider the multicast network depicted in Fig. 2(b). There are in total 20 grey nodes. For every set \( N \) of 3 grey nodes with \( \text{maxflow}(N) = 3 \), there is a receiver connected from it. This network is linearly solvable over every finite field \( \mathbb{GF}(q) \) with \( q \geq q_{\min} = 16 \) except for \( q = q_{\max}^* = 17 \).

A detailed proof of this lemma can be found in [13]. Similar to the case in Fig. 2(a), it can be shown that the network in Fig. 2(b) is linearly solvable over a finite field \( \mathbb{GF}(q) \) if and only if there is an assignment of \( \{\alpha_i, \beta_i\}_{1 \leq i \leq 5}, \{\delta_i\}_{1 \leq i \leq 10} \) from \( \mathbb{GF}(q)^\times \) subject to

\[
\alpha_i \neq \alpha_j, \beta_i \neq \beta_j, \delta_i \neq \delta_j, \quad \forall \ 1 \leq i < j \leq 3,
\]

\[
\{\delta_1, \cdots, \delta_{10}\} \subseteq \mathbb{GF}(q)^\times \{\alpha_i \beta_j : 1 \leq i, j \leq 3\}.
\]

For example, when \( q = 16 \), we can set \( \alpha_i = \beta_i = \xi^3 \) for all \( 1 \leq i \leq 5 \), where \( \xi \) is a primitive element in \( \mathbb{GF}(16) \), and set \( \delta_1, \cdots, \delta_{10} \) to be the 10 elements in \( \mathbb{GF}(16)^\times \{\xi^3 : 1 \leq i \leq 5\} \). Such an assignment satisfies the above condition and hence the network is linearly solvable over \( \mathbb{GF}(16) \). The insight for the network to be linearly solvable over \( \mathbb{GF}(16) \) rather than \( \mathbb{GF}(17) \) is that there is such a subgroup in the multiplicative group \( \mathbb{GF}(16)^\times \) but not in \( \mathbb{GF}(17)^\times \) that (i) the subgroup has order no smaller than 5; (ii) the complement of the subgroup in the multiplicative group contains at least 10 elements.

**Corollary 4.** Given a multicast network with \( q_{\min} < q_{\max}^* \), \( q_{\min} \) can be of either even or odd characteristic.

![Fig. 2](image-url)
III. GAP BETWEEN $q_{\text{min}}$ AND $q_{\text{max}}^*$

To the best of our knowledge, all known multicast networks studied in the network coding literature have the property that $q_{\text{max}}^* < q_{\text{min}}$. The results in the last section reveal that it is possible for $q_{\text{min}} < q_{\text{max}}^*$. However, both examples illustrating this fact have $q_{\text{max}}^* = q_{\text{min}} + 1$. A natural question next is how far away can $q_{\text{max}}^*$ be from $q_{\text{min}}$. The main result in this section is to show that for some multicast networks, the difference $q_{\text{max}}^* - q_{\text{min}}$ can be extremely large.

Consider the Swirl Network\(^1\) with source dimension $\omega \geq 3$ depicted in Fig. 3. For every set $N$ of $\omega$ grey nodes with $\text{max flow}(N) = \omega$, there is a non-depicted receiver connected from it. Corresponding to each node $n_i$ of in-degree 2, where $1 \leq i \leq \omega$, let $d_i, e_i$ denote the two outgoing edges from it. We next derive the necessary and sufficient conditions on $q$ for the Swirl Network to be linearly solvable over $\text{GF}(q)$.

![Swirl Network Diagram](image)

Fig. 3. The Swirl network of source dimension $\omega \geq 3$ has a receiver, which is not depicted, connected from every set $N$ of $\omega$ grey nodes that has $\text{max flow}(N) = \omega$. Corresponding to each node $n_i$ of in-degree 2, $1 \leq i \leq \omega$, let $d_i, e_i$ denote the two outgoing edges from it.

The lemma below can be shown based on the special topology of the Swirl network. Refer to [13] for a detailed proof.

**Lemma 5.** The Swirl network is linearly solvable over a given $\text{GF}(q)$ if and only if there is an LNC over $\text{GF}(q)$ with coding vectors for $\{d_i, e_i\}_{1 \leq i \leq \omega}$ prescribed by

\[
\begin{bmatrix}
    f_{d_1} & f_{e_1} & f_{d_2} & f_{e_2} & \cdots & f_{d_{\omega}} & f_{e_{\omega}} \\
    1 & 1 & 0 & 0 & \cdots & 0 & 0 & 1 & 1 \\
    1 & \alpha_1 & 1 & 1 & \cdots & 0 & 0 & 0 & 0 \\
    0 & 0 & 1 & \alpha_2 & \cdots & 0 & 0 & 0 & 0 \\
    \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\
    0 & 0 & 0 & 0 & \cdots & 1 & 1 & 0 & 0 \\
    0 & 0 & 0 & 0 & \cdots & 1 & \alpha_{\omega-1} & \delta_1 & \delta_2
\end{bmatrix}
\]

\[= \begin{bmatrix}
    1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
    1 & 4 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 1 & 4 & 1 & 1 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 1 & 4 & 1 & 1 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 1 & 4 & 1 & 1 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 2 & 3
\end{bmatrix}, \quad (1)
\]

where

\[
\alpha_1, \cdots, \alpha_{\omega-1}, \delta_1, \delta_2 \in \text{GF}(q)^\times,
\]

$\delta_1 \neq \delta_2$ and $\alpha_j \neq 1$ for all $1 \leq j \leq \omega - 1,$

and

\[
\{\delta_1, \delta_2\} \subseteq \text{GF}(q)^\times \setminus \{(\pm 1)^{\omega} : \gamma_1 \gamma_2 \cdots \gamma_{\omega-1} : \\
\gamma_i \in \{1, \alpha_j\} \text{ for all } 1 \leq j \leq \omega - 1\}. \quad (3)
\]

**Example.** Consider the Swirl network with $\omega = 6$, and an LNC over $\text{GF}(5)$ with the coding vectors for $\{d_1, e_1, \cdots, d_6, e_6\}$ prescribed by

\[
\begin{bmatrix}
    f_{d_1} & f_{e_1} & \cdots & f_{d_6} & f_{e_6} \\
    1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
    1 & 4 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
    0 & 0 & 1 & 4 & 1 & 1 & 0 & 0 & 0 & 0 \\
    0 & 0 & 0 & 0 & 1 & 4 & 1 & 1 & 0 & 0 \\
    0 & 0 & 0 & 0 & 0 & 1 & 4 & 1 & 1 & 0 \\
    0 & 0 & 0 & 0 & 0 & 0 & 1 & 4 & 2 & 3
\end{bmatrix}
\]

Apparently condition (2) is satisfied by this LNC. Since $\{1, 4\}$ is a subgroup of $\text{GF}(5)^\times$, it is closed under multiplication by elements in it. Moreover, $\{2, 3\} = \text{GF}(5)^\times \setminus \{(\pm 1)^6, 1, (\pm 1)^6, 4\}$, condition (3) is also satisfied. Thus, this LNC over $\text{GF}(5)$ qualifies as a linear solution. On the other hand, since $\text{GF}(8)^\times$ does not have a proper subgroup other than $\{1\}$, it is not difficult to check that for arbitrary $\alpha_1, \cdots, \alpha_3 \in \text{GF}(8)^\times \setminus \{1\}$, the set $\{\gamma_1 \gamma_2 \cdots \gamma_3 : \gamma_i \in \{1, \alpha_j\} \text{ for all } 1 \leq i \leq 5\}$ contains at least 6 elements. Thus, there are not enough distinct elements in $\text{GF}(8)^\times$ to assign for $\alpha_1, \cdots, \alpha_3$ and $\delta_1, \delta_2$ subject to conditions (2) and (3). Hence, the network is not linearly solvable over $\text{GF}(8)$.

The argument in the example above can simply be generalized to derive the linear solvability of the Swirl network with general source dimension $\omega$ over a given $\text{GF}(q)$. First, assume that the order of the multiplicative group $\text{GF}(q)^\times$ is not prime. This implies $q \geq 5$. Then there is a subgroup $G$ in $\text{GF}(q)^\times$ with $|G| \geq 2$, and $\text{GF}(q)^\times \setminus \{(\pm 1)^q : g \in G\}$ contains no less than 2 elements. Let $a$ be an element in $G$ not equal to 1 and $b, c$ be two distinct elements in $\text{GF}(q)^\times \setminus \{(\pm 1)^g : g \in G\}$. We can assign $\alpha_i = a$ for all $1 \leq i \leq \omega - 1$ and $\delta_1 = b, \delta_2 = c$. Such an assignment obeys conditions (2) and (3). Hence, the network is linearly solvable over $\text{GF}(q)$.

\[1\text{The name is due to both the shape of the network and the close connection to a matroid structure referred to as the free swirl (See Chapter 14 in [15].)}\]
$2^p - 2$, the set \( \{ \gamma_1 \cdots \gamma_{w-1} : \gamma_i \in \{1, \xi^i\} \} \) contains at least \( \omega \) elements. In order to further successfully assign \( \delta_1, \delta_2 \) subject to (2) and (3), the size of \( GF(2^p) \) has to be at least \( \omega + 3 \). We have proved the following theorem.

**Theorem 6.** The Swirl network with \( \omega \geq 3 \) has \( q_{\text{min}} = 5 \). It is not linearly solvable over those \( GF(2^p) \) when \( 2^p \leq \omega + 2 \) and \( 2^p - 1 \) is a prime.

Recall that a prime integer in the form \( 2^p - 1 \) is known to be a *Mersenne prime*. Then \( q_{\text{max}}^* \) for the Swirl network with \( \omega \geq 3 \) is equal to one plus the largest Mersenne prime no larger than \( \omega + 1 \). While whether there are infinitely many Mersenne primes is still an open problem, the \( 48^{th} \) known Mersenne prime (which is also the largest known prime) found under the GIMPS project (See [16]) has a length of 17,425,170 digits under base 10. Thus, when \( \omega \) is sufficiently large, the difference \( q_{\text{max}}^* - q_{\text{min}} \) for the Swirl network is so enormous as to having tens of millions of digits.

**Corollary 7.** If there are infinitely many Mersenne primes, then there are infinitely many multicast networks with \( q_{\text{max}}^* > q_{\text{min}} \), and moreover, the difference \( q_{\text{max}}^* - q_{\text{min}} \) can tend to infinity.

**IV. Summary**

In an acyclic multicast network, if there is a linear solution over \( GF(q) \), could we claim that there is a linear solution over every \( GF(q') \) with \( q' \geq q \)? It would be tempting to answer it positively because by the result in [5], the claim is correct when \( q \) is no smaller than the number of receivers and moreover, as a consequence of the result in [7], the positive answer is affirmed for the special case that the source dimension of the network is equal to 2. In the present paper, however, we show the negative answer for general cases by constructing several classes of multicast networks with different emphasis. These networks are the first ones discovered in the network coding literature with the property that \( q_{\text{max}}^* \) the maximum field size for the nonexistence of a linear solution over \( GF(q_{\text{max}}^*) \), is larger than \( q_{\text{min}} \), the minimum field size for the existence of a linear solution over \( GF(q_{\text{min}}) \). The insight of various exemplifying networks established in the present paper is that not only the field size of \( GF(q) \), but also the order of the proper multiplicative subgroup of \( GF(q)^\times \) affects the networks’ linear solvability over \( GF(q) \).

The results in this paper bring about a new thread on the fundamental study of linear network coding. We end this paper by proposing a number of open problems:

- For a multicast network, what is the smallest prime power \( q \) larger than \( q_{\text{max}}^* \) (such that the network is linearly solvable over all \( GF(q') \) with \( q' \geq q \))?
- Can the gap \( q_{\text{max}}^* - q_{\text{min}} > 0 \) tend to infinity?
- Are there infinitely many prime power pairs \((q, q')\) with \( q < q' \) such that each \((q, q')\) corresponds to \((q_{\text{min}}, q_{\text{max}}^*)\) of some multicast network?
- If a multicast network is linearly solvable over such a \( GF(q) \) that \( GF(q)^\times \) does not contain any proper multiplicative subgroup other than \( \{1\} \), is it linearly solvable over all larger finite fields than \( GF(q) \)?
- If a multicast network is linearly solvable over \( GF(2) \), is it linearly solvable over all finite fields?
- If a multicast network is linearly solvable over both \( GF(2) \) and \( GF(3) \), is it linearly solvable over all finite fields?

**ACKNOWLEDGMENT**

The authors would like to thank Sidharth Jaggi for helping identify and motivate the problem studied in this work.

**REFERENCES**


