Finite Fields and Their Applications 46 (2017) 65–89

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On the girth of Tanner (3, 11) quasi-cyclic LDPC codes ☆

Hengzhou Xu [a,b], Baoming Bai [b,*], Dan Feng [b], Cheng Sun [b]

[a] *School of Network Engineering, Zhoukou Normal University, Zhoukou 466001, China*

[b] *State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China*

A R T I C L E   I N F O

Article history:
Received 15 December 2015
Received in revised form 6 August 2016
Accepted 1 March 2017
Available online xxxx
Communicated by Xiang-Dong Hou

MSC:
94B05
94B15

Keywords:
Finite field
Quasi-cyclic (QC) LDPC codes
Girth
Tanner graph

A B S T R A C T

Motivated by the works on the girth of Tanner $(3, 5)$ and $(3, 7)$ quasi-cyclic (QC) low-density parity-check (LDPC) codes done by S. Kim et al. and M. Gholami et al., respectively, we analyze the cycles of Tanner $(3, 11)$ QC LDPC codes and present the sufficient and necessary conditions for the existence of cycles of lengths 4, 6, 8, and 10 in Tanner $(3, 11)$ QC LDPC codes. By checking these conditions, the girth values of Tanner $(3, 11)$ QC LDPC codes are derived.

☆ This work was supported in part by the National Natural Science Foundation of China under Grants 61372074 and 91438101, the 973 Program of China under Grant 2012CB316100, and the Joint Funds of the National Natural Science Foundation of China under Grant U1504601.

* Corresponding author.

E-mail addresses: hzxu@zknu.edu.cn (H. Xu), bmbai@mail.xidian.edu.cn (B. Bai), dfeng_14@stu.xidian.edu.cn (D. Feng), chengsun@stu.xidian.edu.cn (C. Sun).

http://dx.doi.org/10.1016/j.ffa.2017.03.004

1. Introduction

LDPC codes were invented by Gallager in 1960s [5] and were redescribed by Tanner in 1981 [17]. In 1990s, it was discovered that LDPC codes could achieve performance extremely close to Shannon capacity [12]. Since then a great deal of research effort has been made on construction, encoding, decoding, and performance analysis of LDPC codes [3,7,14,15,18,20]. Especially, the work on construction of LDPC codes is significant. Based on the construction methods, LDPC codes could be classified into two major categories: (1) random-like codes constructed by computer search [8]; and (2) structured codes based on mathematical tools [16], such as finite field [11], combinational designs [10], and graph theory [19]. In the hardware implementation aspect, structured LDPC codes, especially quasi-cyclic (QC) LDPC codes [1,4], can be encoded in linear time using shift registers. The corresponding decoder requires much smaller memory space to store the parity-check matrix and less computations than that of the random-like codes. Notice that some good structured LDPC codes can also be contained in generalized quasi-cyclic (GQC) codes [13]. Furthermore, for short to medium lengths, QC LDPC codes can perform better than the random-like ones [4]. Therefore, many QC LDPC codes have found applications in data storage and communication systems. Note that in data storage and optical communication applications, much higher coding rate is required, and large coding gain and very low probability of block error are also necessary [2]. It has been demonstrated that structured high-rate LDPC codes with larger girth can achieve good error-floor performance. Tanner $(3, 11)$ QC LDPC codes are a class of such LDPC codes, whose rate is about 0.33 and 0.16 higher than that of Tanner $(3, 5)$ QC LDPC [9] and Tanner $(3, 7)$ QC LDPC [6] codes, respectively.

A QC LDPC code is defined by the null space of its parity-check matrix $\mathbf{H}$ which is a sparse array of circulant matrices. If each column weight and row weight of $\mathbf{H}$ is a constant, denoted by γ and ρ respectively, the null space of $\mathbf{H}$ gives a (γ, ρ)-regular QC LDPC code. In [4], Fossorier proposed a class of QC LDPC codes whose parity-check matrices are composed of γ rows of ρ circulant permutation matrices (CPMs). He analyzed the cycles of this class of (γ, ρ)-regular QC LDPC codes and gave the necessary conditions for the existence of cycles of lengths 4, 6, 8, and 10. Therefore, he presented a sufficient and necessary condition for this class of QC LDPC codes to have a girth at least $2(i + 1), i \in N^*$. In [4], it is also proved that the girths of this class of QC LDPC codes are less than or equal to twelve. Based on this result, the girths of a class of QC LDPC codes proposed by Tanner et al. [17], called Tanner QC LDPC codes in this paper, are at most twelve. S. Kim, et al. showed that the girth of Tanner $(3, 5)$ QC LDPC codes of length $5p$, where p is a prime of the form $15m + 1$, is 8 if $p = 31$, the girth is 10 if $p = 61, 151$, the girth is 12 in the other cases [9]. Subsequently, M. Gholami et al. derived the girth values of Tanner $(3, 7)$ QC LDPC codes of length $7p$ with p being a prime of the form $21m+1$. Namely, the girth of Tanner $(3, 7)$ QC LDPC codes is 8 if $p = 43, 127$, the girth is 10 if $p = 211, 337, 379, 421, 463, 547, 631, 757, 1429, 2437, 3109$, and the girth is 12 in the remaining cases [6]. Actually, they analyzed the cycles of Tanner $(3, 5)$ QC