Journal of Algebraic Systems
Vol. 8, No. 2, (2021), pp 283-289

4-CYCLE FREE APM-LDPC CODES WITH AN EXPLICIT CONSTRUCTION

Z. GHOLAMI AND M. GHOLAMI*

Abstract. Recently, attention has been focused on a class of low-density parity-check codes from *affine permutation matrices*, called APM-LDPC codes, having some advantages than quasi-cyclic (QC) LDPC codes in terms of minimum-distance, cycle distribution and error-rate performance. Moreover, some explicit constructions for exponent matrices of conventional APM-LDPC codes with girth at least 6 have been investigated. In this paper, a class of 4-cycle free APM-LDPC codes is constructed by a new explicit method such that the constructed codes have better cycle distributions rather than the recently proposed APM codes with girth 6. As simulation results show, the constructed codes outperform PEG and random-like LDPC codes with the same rates and lengths.

1. Preliminaries

For given positive integer m, let $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ be the ring of integers modulo m and $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m | \gcd(a, m) = 1\}$ be the set of elements in $\mathbb{Z}_m$ which are relatively prime to m. Now, for each $(s, a) \in \mathbb{Z}_m \times \mathbb{Z}_m^*$, define affine permutation (AP) matrix $\mathcal{I}_m^{s,a}$, briefly $\mathcal{I}^{s,a}$ when m is known, to be the $m \times m$ binary matrix $(p_{i,j})_{0 \le i,j \le m-1}$ in which $p_{i,j} = 1$ if and only if $i = aj + s \bmod m$. In fact, in $\mathcal{I}^{s,a}$, the row-index of 1 in the first column is s and each column is shifted down

DOI: 10.22044/jas.2020.9086.1441.
MSC(2010): Primary: 11H71; Secondary: 68P30, 11Y50.
Keywords: APM-LDPC codes, explicit constructions, girth.
Received: 1 November 2019, Accepted: 24 May 2020.
*Corresponding author.

by a respect to the previous column. Some of the properties of AP matrices can be seen easily as follows [3].

(1) $\mathcal{I}^{s_1,a_1} \times \mathcal{I}^{s_2,a_2} = \mathcal{I}^{s_1+a_1s_2,a_1a_2}$.
(2) $\mathcal{I}^{s_1,a_1}/\mathcal{I}^{s_2,a_2} = \mathcal{I}^{s_1-s_2a_1a_2^{-1},a_1a_2^{-1}}$.
(3) $(\mathcal{I}^{s,a})^{-1} = (\mathcal{I}^{s,a})^T = \mathcal{I}^{-sa^{-1},a^{-1}}$.
(4) $(\mathcal{I}^{s,a})^n = \begin{cases} \mathcal{I}^{s\frac{a^n-1}{a-1},a^n} & a \neq 1 \\ \mathcal{I}^{sn,1} & a = 1 \end{cases}$

By the above relations, it is clear that the set of all APMs of size m, i.e. $\{I^{s,a} : (s,a) \in \mathbb{Z}_m \times \mathbb{Z}_m^*\}$, with the multiplication operation, forms a non-abelian group of order $m \times \phi(m)$, where $\phi(m) = |\mathbb{Z}_m^*|$ is the phi-Euler's function.

Now, for a given $J \times L$ fully-one matrix B, let $E = (e_{i,j})_{0 \leq i \leq J-1, 0 \leq j \leq L-1}$ be a $J \times L$ array on $\mathbb{Z}_m \times \mathbb{Z}_m^*$, i.e. each element $e_{i,j}$ is a pair $(s_{i,j}, a_{i,j}) \in \mathbb{Z}_m \times \mathbb{Z}_m^*$. The (J, L) APM-LDPC code with base matrix B, APM-size m and exponent matrix E can be defined as an LDPC code having the following parity-check matrix.

$$\mathcal{H}_{m,E} = \begin{pmatrix} \mathcal{I}^{s_{0,0},a_{0,0}} & \cdots & \mathcal{I}^{s_{0,L-1},a_{0,L-1}} \\ \vdots & \ddots & \vdots \\ \mathcal{I}^{s_{J-1,0},a_{J-1,0}} & \cdots & \mathcal{I}^{s_{J-1,L-1},a_{J-1,L-1}} \end{pmatrix} \tag{1.1}$$

In the literature, the $J \times L$ matrices $S = (s_{i,j})_{0 \leq i \leq J-1, 0 \leq j \leq L-1}$ and $A = (a_{i,j})_{0 \leq i \leq J-1, 0 \leq j \leq L-1}$ are called *slope* and *shift* matrices, respectively. It is noticed that, if an element of E is greater than m, in construction of $\mathcal{H}_{m,E}$, such element is considered to be modulo m. Especially, if $a_{i,j} = 1$ for each $0 \leq i \leq J-1$ and $0 \leq j \leq L-1$, then $\mathcal{H}_{m,E}$ in (1.1) can be considered as the parity-check matrix of a QC-LDPC code with circulant permutation matrix (CPM) size m. Moreover, after some elementary row (column) operations on $\mathcal{H}_{m,E}$, it may be considered as the parity-check matrix of a QC-LDPC code. The following theorem gives a necessary condition such that $\mathcal{H}_{m,E}$ is the parity-check matrix of a QC-LDPC code.

Theorem 1.1. *If* $(s_i^{(r)}, a_i^{(r)}) \in \mathbb{Z}_m \times \mathbb{Z}_m^*$, $0 \leq i \leq J-1$, *and* $(s_j^{(c)}, a_j^{(c)}) \in \mathbb{Z}_m \times \mathbb{Z}_m^*$, $0 \leq j \leq L-1$, *are given such that for each* i, j, $a_i^{(r)} a_j^{(c)} a_{i,j} = 1 \bmod m$, *then* $\mathcal{H}_{m,E}$ *can be considered as the parity-check matrix of a QC-LDPC code.*

Proof. For $0 \leq i \leq J-1$ and $0 \leq j \leq L-1$, multiplying the ith row-block of $\mathcal{H}_{m,E}$ by $\mathcal{I}^{(s_i^{(r)}, a_i^{(r)})}$ and then multiplying the jth column-block of $\mathcal{H}_{m,E}$ by $\mathcal{I}^{(s_j^{(c)}, a_j^{(c)})}$, the matrix $\mathcal{H}_{m,E'}$ with exponent matrix

$E' = (e'_{i,j})$, will be obtained, in which

$$e'_{i,j} = \left((a_i^{(r)} s_{i,j} + s_i^{(r)}) a_j^{(c)} + s_j^{(c)}, a_i^{(r)} a_j^{(c)} a_{i,j}\right) \in \mathbb{Z}_m \times \mathbb{Z}_m^*.$$

Now, if $a_i^{(r)} a_j^{(c)} a_{i,j} = 1$, for each i, j, then $\mathcal{H}_{m,E'}$ is the parity-check matrix of a QC-LDPC code and the proof is completed. □

Example 1.2. For given positive integers J and L, and prime number m, $m > JL$, the matrix $A = (a_{i,j})$, $a_{i,j} = (i+1)(j+1)$, $0 \leq i \leq J-1$, $0 \leq j \leq L-1$, can be considered as a $(J, L)-$shift matrix of an APM-LDPC code $\mathcal{C}$, because for each i, j we have $\gcd(a_{i,j}, m) = 1$. Now, substituting $a_i^{(r)} = (i+1)^{-1} \pmod{m}$ and $a_j^{(c)} = (j+1)^{-1} \pmod{m}$ in Theorem 1.1, we have $a_i^{(r)} a_j^{(c)} a_{i,j} = 1 \pmod{m}$, and so $\mathcal{C}$ is equivalent to a QC-LDPC code.

The following theorem gives a necessary and sufficient condition for the existence of a $2l-$cycle in the Tanner graph of a (J, L) APM-LDPC code with the parity-check matrix $\mathcal{H}_{m,E}$.

Theorem 1.3. ([3]) A $2l$-cycle in $\mathrm{TG}(\mathcal{H}_{m,E})$ exists if and only if there is a chain (i_0, j_0); (i_1, j_1); $\cdots$; (i_{l-1}, j_{l-1}); $(i_l, j_l) = (i_0, j_0)$, $0 \leq i_k \neq i_{k+1} \leq J-1$ and $0 \leq j_k \neq j_{k+1} \leq L-1$, such that one of the following relations holds:

(1) $p_0 = 1$ and $A = 0$.
(2) $\gcd(p_0 - 1, m) | A$.

in which $p_h = \prod_{k=h}^{l-1} a_{i_{k+1},j_k} a_{i_k,j_k}^{-1} \bmod m$, $0 \leq h \leq l-1$, $p_l = p_0$, and $A = \sum_{k=0}^{l-1} (p_k s_{i_k,j_k} - p_{k+1} s_{i_{k+1},j_k}) \bmod m$.

In particular case, if $l = 2$, then Theorem 1.3 can be summarized as follows.

Corollary 1.4. $\mathrm{TG}(\mathcal{H}_{m,E})$ is free of 4-cycles if and only if for each $0 \leq i_0 < i_1 < J-1$ and $0 \leq j_0 < j_1 < L-1$, we have $v \neq 0$ if $u = 0$ or otherwise $\gcd(u, m) \nmid v$, in which $u = a_{i_1,j_0} a_{i_0,j_1} - a_{i_1,j_1} a_{i_0,j_0} \bmod m$ and $v = a_{i_0,j_1} a_{i_1,j_0} (s_{i_0,j_0} - s_{i_0,j_1}) + a_{i_0,j_0} a_{i_0,j_1} (s_{i_1,j_1} - s_{i_1,j_0}) \bmod m$.

Proof. Setting $l = 2$ in Theorem 1.3, we have $p_0 = a_{i_1,j_0} a_{i_0,j_0}^{-1} a_{i_0,j_1} a_{i_0,j_1}^{-1} \bmod m$ and $A = a_{i_1,j_0} a_{i_0,j_0}^{-1} a_{i_0,j_1} a_{i_0,j_1}^{-1} (s_{i_0,j_0} - s_{i_0,j_1}) + a_{i_0,j_1} a_{i_0,j_1}^{-1} (s_{i_1,j_1} - s_{i_1,j_0}) \bmod m$. On the other hand, by the proof of Theorem 1.3 in [3], the existence of a 4-cycle in $\mathrm{TG}(\mathcal{H})$ is related to the resolvability of the equation $(p_0 - 1)x = A \bmod m$, which can be solved if and only if $a_{i_0,j_0} a_{i_1,j_1} (p_0 - 1)x = a_{i_0,j_0} a_{i_1,j_1} A \pmod{m}$ is resolvable, because $\gcd(a_{i_0,j_0} a_{i_1,j_1}, m) = 1$. Now, this equation is simplified as $ux = v$

(mod m) which has no solution if and only if $v \neq 0$ and $u = 0$ or $\gcd(u, m) \nmid v$. □

Cycles, especially cycles of length 4, in the Tanner graph of an LDPC code degrade the performance of LDPC decoders. Therefore, design of LDPC codes free of 4-cycles is of great interest. Here, for enough large m, we give some exponent matrices E explicitly such that $\mathcal{H}_{m,E}$ has girth 6. In fact, an exponent matrix E is constructed explicitly with the lower-bound $Q(E)$, such that $g(\mathcal{H}_{m,E}) \geq 6$ for each $m \geq Q(E)$.

2. Explicit Constructions of APM-LDPC Codes with Girth at Most 6

In order to construct APM-LDPC codes with girth 6, we start from the following theorem. Before that, for positive integers m and prime p, define $\nu_p(m)$ to be the largest power of p which divides m, i.e. $\nu_p(m) = e$ if and only if $p^e | m$ and $p^{e+1} \nmid m$. Clearly, for two integers a, b, we have $\nu_p(ab) = \nu_p(a) + \nu_p(b)$, so $\nu_p(p^k a) = k + \nu_p(a)$, $\nu_p((kp+1)a) = \nu_p(a)$ and if $a|b$, then $v_p(a) \leq v_p(b)$. Moreover, by the Legendre's formula [13] for the factorial of an integer number, we have $\nu_p(m!) = \sum_{i=1}^{\infty} \left\lfloor \frac{m}{p^i} \right\rfloor$, where $\lfloor x \rfloor$ is the floor function. Moreover, for each integer $m = 1 \times 3 \times 5 \times \cdots \times (2N-1)$, we have $\nu_p(m) = \nu_p((2N)!) - \nu_p(N!)$.

Theorem 2.1. For prime p and integers J, L, $J < L$, let $E = (e_{i,j})$, be a $(J, L)-$exponent matrix, such that $e_{i,j} = (s_{i,j}, a_{i,j})$, in which $s_{i,j} = ij$ and $a_{i,j} = (i+j)p + 1$, $0 \leq i \leq J-1$ and $0 \leq j \leq L-1$. Then, for each $m = p^k$, $k > \log_p (J-1)(L-1)$, we have $g(\mathcal{H}_{m,E}) \geq 6$.

Proof. Substituting $s_{i,j}$ and $a_{i,j}$ in Corollary 1.4, we have $u = p^2(j_1 - j_0)(i_1 - i_0) \bmod m$ and $v = (i_0 - i_1)(j_0 - j_1)(kp+1) \bmod m$, where $k = (i_0 j_0 + j_0 j_1)p + i_0 + j_0 + j_1$. Set $e = \nu_p((j_1 - j_0)(i_1 - i_0))$. Now, if $e < k-2$, then $u \neq 0$, because $\nu_p(u) = e + 2 < \nu_p(m) = k$ and $(j_1 - j_0)(i_1 - i_0) \neq 0$. In this case, $\gcd(u, m) = p^{e+2}$ which is not divisible by v, because $\nu_p(v) = \nu_p((j_1 - j_0)(i_1 - i_0)) = e < e+2 = \nu_p(\gcd(u, m))$. On the other hand, if $e \geq k-2$, then $u = 0$, but $v \neq 0$, because $v = 0$ if and only if $(j_1 - j_0)(i_1 - i_0) = 0 \bmod m$. However, $(j_1 - j_0)(i_1 - i_0) \neq 0 \bmod m$, because $0 < (j_1 - j_0)(i_1 - i_0) \leq (J-1)(L-1) < p^k = m$. □

It is worth noticing that the APM-LDPC code constructed by Theorem 2.1 is not equivalent to a QC-LDPC code, because by Theorem 1.1, the expression $\frac{1}{(i+j)p+1}$ can not be decomposed to the multiplications of two functions in terms of the variables i and j. On the other hand, $a_{i,j} = (i+j)p + 1$ is always prime respect to $m = p^k$, for each i, j.

v	k	m	$n_{6,8}$	m_1 [12]	$n_{6,8}$	m_2 [4]	$n_{6,8}$	m_3 [5]	$n_{6,8}$
3	5	16	744	16	1192	17	850	16	888
	6	16	1856	16	2432	17	1938	16	1952
	7	16	3832	16	4568	17	3859	16	3928
	8	16	7008	16	7904	17	6817	16	7200
4	5	16	3232	16	3984	17	3604	16	3536
	6	16	7760	16	8800	17	8446	16	8144
	7	16	16112	16	17040	17	16439	16	16400
	8	16	29540	16	30528	17	29529	16	29952
5	6	32	23808	32	37536	31	25296	32	29472
	7	32	49232	32	68336	31	50623	32	56816
	8	32	89600	32	113344	31	91729	32	97088

Table 1. A comparison between the number of 6,8-cycles of the constructed codes with some explicit QC, APM and AQC-LDPC codes in [12], [4] and [5]

Example 2.2. For $p = 5$, let E be the following 5×7 exponent matrix given by Theorem 2.1.

$$\begin{pmatrix} (0,1) & (0,6) & (0,11) & (0,16) & (0,21) & (0,26) & (0,31) \\ (0,6) & (1,11) & (2,16) & (3,21) & (4,26) & (5,31) & (6,36) \\ (0,11) & (2,16) & (4,21) & (6,26) & (8,31) & (10,36) & (12,41) \\ (0,16) & (3,21) & (6,26) & (9,31) & (12,36) & (15,41) & (18,46) \\ (0,21) & (4,26) & (8,31) & (12,36) & (16,41) & (20,46) & (24,51) \end{pmatrix}$$

For $k \geq \lceil \log_5 (5-1)(7-1) \rceil = 2$, we have $g(\mathcal{H}_{m,E}) \geq 6$. It is note that each element of E is reduced in modulo m. For example, for $m = 25$, the element $(24, 51)$ in the above exponent matrix is reduced to $(24, 1)$.

3. OUTPUTS

Table 1 provides some comparisons between the 6,8-cycle multiplicities of the constructed codes with block-size m, on one hand, and some QC-LDPC codes [12] with CPM-size m_1, APM-LDPC codes [4] with APM-size m_2 and AQC-LDPC codes [5] with block size m_3 with some explicit constructions, on the other hand. All of the codes considered in this comparison have girth at least 6. In the table, $n_{6,8}$ is the summation of 6,8 cycle multiplicities of the corresponding codes. As Table 1 shows, the constructed codes have better $n_{6,8}$ rather than QC and AQC-LDPC codes, although, they have a close comparisons with the APM-LDPC codes in [4].

4. SIMULATION RESULTS

For simulation results, we have used an additive white Gaussian noise (AWGN) channel, using software available online [7]. The decoding algorithm is sum-product with iteration number 50 and block number 1000. Figure 1 shows a bit error performance comparison between two

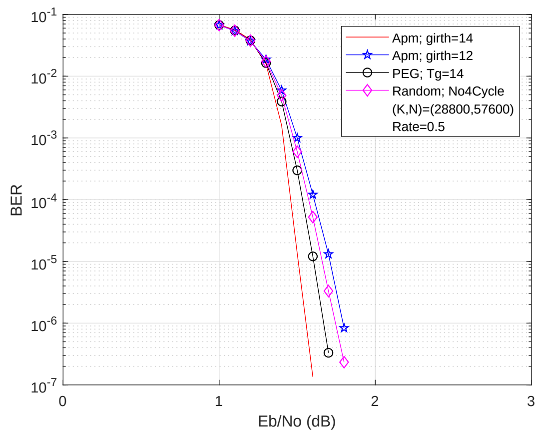

FIGURE 1. The constructed APM codes with different girths against Random and PEG LDPC codes

QC-LDPC codes with different girths having lifting degree 9600 lifted from the base matrix of the $(3, 6)$ APM-LDPC code constructed explicitly, on one hand and a 4-cycle free randomly constructed LDPC code and an LDPC code from progressive edge growth (PEG) [9] with target girth 14, on the other hand. As the figure confirms, the constructed codes outperform random and PEG codes with the same lengths, rates and girths.

Acknowledgments

This work was supported in part by the research council of Shahrekord University.

References

1. I. E. Bocharova, F. Hug, R. Johannesson, B. D. Kudryashov and R. V. Satyukov, Searching for voltage graph-based LDPC tailbiting codes with large girth, *IEEE Trans. Inf. Theory*, **58** (2012), 2265–2279.
2. M. David, R. Smarandache and D. J. Costello, Quasi-cyclic LDPC codes based on pre-lifted protographs, *IEEE Trans. Inf. Theory*, **60** (2014), 5856–5874.
3. M. Gholami and M. Alinia, High-performance binary and nonbinary LDPC codes based on affine permutation matrices, *IET Commun.*, **9** (2015), 2114–2123.
4. M. Gholami and M. Alinia, Explicit APM-LDPC codes with girths 6, 8, and 10, *IEEE Signal Processing Lett. 24* (2017), 741–745.
5. Z. Gholami and M. Gholami, Anti Quasi-Cyclic LDPC Codes, *IEEE Commun. Lett.*, **22** (2018), 1116–1119.
6. M. Gholami and A. Nassaj, Row and column extensions of 4-cycle free LDPC codes, *IEEE Commun. Lett.*, **20** (2016), 25– 28.
7. http://www.cs.utoronto.ca/ radford/ldpc.software.html.

8. ⟨http : //www.cs.toronto.edu/Radford/ldpc.software.html⟩.
9. X.-Y. Hu, E. Eleftheriou and D. M. Arnold, Regular and irregular progressive edge-growth Tanner graphs, *IEEE Trans. Inf. Theory*, **51** (2005) 386–398.
10. C.-M. Huang, J.-F. Huang, and C.-C. Yang, Construction of quasi-cyclic LDPC codes from quadratic congruences, *IEEE Commun. Lett.*, **12** (2008), 313–315.
11. J. Huang, L. Liu, W. Zhou and S. Zhou, Larg-girth nonbinary QC-LDPC codes of various lengths, *IEEE Trans. Commun.*, **58** (2010), 3436–3447.
12. M. Karimi and A. H. Banihashemi, On the girth of quasi cyclic protograph LDPC codes, *IEEE. Trans. Inf. Theory*, **59** (2013), 4542–4552.
13. A. M. Legendre, Th orie des Nombres, Paris: Firmin Didot Fr res, 1830.
14. L. Liu and W. Y. Zhou, Design of QC-LDPC code with continuously variable length, *J. Elect. Inf. Tech.*, **31** (2009), 2523–2526.
15. D. J. C. MacKay, Good error-correcting codes based on very sparse matrices, *IEEE Trans. Inf. Theory*, **45** (1999), 399–431.
16. S. Myung and K. Yang, A combining method of quasi-cyclic LDPC codes by the chinese remainder theorem, *IEEE Commun. Lett.*, **9** (2005), 823 –825.
17. R. M. Tanner, On graph constructions for LDPC codes by quasi-cyclic extension, *Information, Coding and Mathematics*, The Springer International Series in Engineering and Computer Science, Springer, Boston, **687** (2002), 209–220.
18. J. Wang, G. Zhang and Q. Zhou, Coset-based QC-LDPC codes without small cycles, *Elect. Lett.*, **50** (2014), 1597–1598.
19. K. Yang and S. Myung, A combining method of quasi-cyclic LDPC codes by the Chinese remainder theorem, *IEEE Commun. Lett.*, **9** (2005), 823–825.
20. Q. Zhang, X. Li, D. Zhang and B. Guo, Regular quasi-cyclic LDPC codes with girth 6 from prime fields, *Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP)*, (2010), 470–473.
21. G. Zhang, R. Sun, and X. Wang, Several explicit constructions for $(3, L)$ QC-LDPC codes with girth at least eight, *IEEE Commun. Lett.*, **17** (2013), 1822–1825.
22. G. Zhang, R. Sun and X. Wang, Construction of girth-eight QC-LDPC codes from greatest common divisor, *IEEE Commun. Lett.*, **17** (2013), 369–372.
23. J. Zhang and G. Zhang, Deterministic girth-eight QC-LDPC codes with large column weight, *IEEE Commun. Lett.*, **18** (2014), 656–659.

Zahra Gholami
Department of Mathematics, University of Shahrekord, P.O. Box 8818634141, Shahrekord, Iran.
Email: `zghbaba123@gmail.com`

Mohammad Gholami
Department of Mathematics, University of Shahrekord, P.O. Box 8818634141, Shahrekord, Iran.
Email: `gholami-m@sci.sku.ac.ir`, `gholamimoh@gmail.com`

Journal of Algebraic Systems

4-CYCLE FREE APM-LDPC CODES WITH AN EXPLICIT CONSTRUCTION

Z. GHOLAMI AND M. GHOLAMI

کدهای خلوت آفین فاقد دور به طول ۴ با یک ساختار صریح

زهرا غلامی[۱] و محمد غلامی[۲]

[۱،۲] دانشکده علوم ریاضی، دانشگاه شهرکرد، شهرکرد، ایران

اخیراً، دسته ای از کدهای با ماتریس بررسی توازن کم‌چگال (کدهای خلوت) بر پایه ماتریس‌های جایگشتی آفین به نام کدهای آفین مورد توجه قرار گرفته‌اند که نسبت به کدهای خلوت شبه‌دوری دارای مزایایی بر حسب کمترین-فاصله، توزیع دوری و کارآیی نرخ خطا می‌باشند. علاوه براین، برخی ساختارهای صریح برای ماتریس‌های توانی کدهای خلوت آفین متعارف (فاقد بلوک صفر در ماتریس بررسی توازن) با کمر حداقل ۶ مطرح شده است. در این مقاله، دسته‌ای از کدهای خلوت آفین فاقد دور به طول ۴ با استفاده از یک روش صریح ساخته می‌شوند که نسبت به کدهای آفین با کمر ۶ مطرح شده در سال‌های اخیر دارای توزیع دوری مناسب‌تری می‌باشند. همان‌گونه که نتایج شبیه‌سازی نشان می‌دهد، کدهای ساخته شده نسبت به کدهای تصادفی و کدهای PEG با طول و نرخ مشابه، دارای کارآیی نرخ خطای بهتری می‌باشند.

کلمات کلیدی: کدهای خلوت آفین، ساختارهای صریح، کمر.