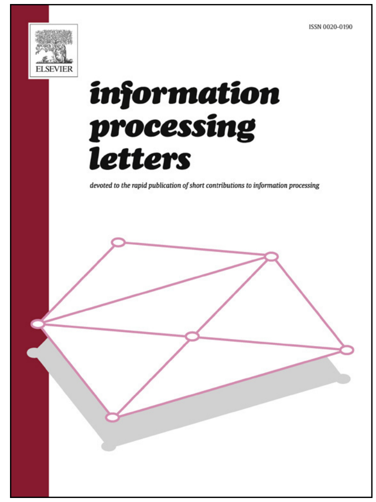

New lower bound on the Shannon capacity of C_7 from circular graphs

Sven Polak, Alexander Schrijver

PII: S0020-0190(18)30229-1
DOI: https://doi.org/10.1016/j.ipl.2018.11.006
Reference: IPL 5764

To appear in: *Information Processing Letters*

Received date: 22 August 2018
Revised date: 13 November 2018
Accepted date: 13 November 2018

Highlights

- An independent set of size 367 is given in the fifth strong product power of C_7.
- This leads to an improved lower bound on the Shannon capacity of C_7: $\Theta(C_7) \geq 367^{1/5} > 3.2578$.
- The independent set is found by computer, using circular graphs.
- It is used that $t \cdot (1, 7, 7^2, 7^3, 7^4) \mid t \in Z_{382} \subseteq Z_{382}^5$ is independent in $C_{108,382}^5$.

New lower bound on the Shannon capacity of C_7 from circular graphs

Sven Polak[1] and Alexander Schrijver[1]

Abstract. We give an independent set of size 367 in the fifth strong product power of C_7, where C_7 is the cycle on 7 vertices. This leads to an improved lower bound on the Shannon capacity of C_7: $\Theta(C_7) \geq 367^{1/5} > 3.2578$. The independent set is found by computer, using the fact that the set $\{t \cdot (1, 7, 7^2, 7^3, 7^4) \mid t \in \mathbb{Z}_{382}\} \subseteq \mathbb{Z}_{382}^5$ is independent in the fifth strong product power of the circular graph $C_{108,382}$. Here the circular graph $C_{k,n}$ is the graph with vertex set $\mathbb{Z}_n$, the cyclic group of order n, in which two distinct vertices are adjacent if and only if their distance (mod n) is strictly less than k.

Keywords: Shannon capacity, independent set, circular graph, cube packing
MSC 2010: 05C69, 94A24

1 Introduction

For any graph $G = (V, E)$, let G^d denote the graph with vertex set V^d and edges between two distinct vertices $(u_1, \ldots, u_d)$ and $(v_1, \ldots, v_d)$ if and only if for all $i \in \{1, \ldots, d\}$ one has either $u_i = v_i$ or $u_i v_i \in E$. The graph G^d is known as the d-th *strong product power* of G. The *Shannon capacity* of G is

$$\Theta(G) := \sup_{d \in \mathbb{N}} \sqrt[d]{\alpha(G^d)}, \tag{1}$$

where $\alpha(G^d)$ denotes the maximum cardinality of an independent set in G^d, i.e., a set of vertices no two of which are adjacent. As $\alpha(G^{d_1+d_2}) \geq \alpha(G^{d_1})\alpha(G^{d_2})$ for any two positive integers d_1 and d_2, by Fekete's lemma [6] it holds that $\Theta(G) = \lim_{d\to\infty} \sqrt[d]{\alpha(G^d)}$.

The Shannon capacity was introduced by Shannon [13] and is an important and widely studied parameter in information theory (see e.g., [1, 4, 9, 11, 15]). It is the effective size of an alphabet in an information channel represented by the graph G. The input is a set of letters $V = \{0, \ldots, n-1\}$ and two letters are confusable when transmitted over the channel if and only if there is an edge between them in G. Then $\alpha(G)$ is the maximum size of a set of pairwise non-confusable single letters. Moreover, $\alpha(G^d)$ is the maximum size of a set of pairwise non-confusable d-letter words. Taking d-th roots and letting d go to infinity, we find the effective size of the alphabet in the information channel: $\Theta(G)$.

The Shannon capacity of C_5, the cycle on 5 vertices, was already discussed by Shannon in 1956 [13]. It was determined more than twenty years later by Lovász [11] using his famous ϑ-function. He proved that $\Theta(C_5) = \sqrt{5}$. The easy lower bound is obtained from the independent set $\{(0,0), (1,2), (2,4), (3,1), (4,3)\}$ in C_5^2 and the ingenious upper bound is given by Lovász's ϑ-function. More generally, for odd n,

$$\Theta(C_n) \leq \vartheta(C_n) = \frac{n\cos(\pi/n)}{1 + \cos(\pi/n)}. \tag{2}$$

[1]Korteweg-De Vries Institute for Mathematics, University of Amsterdam. E-mail: s.c.polak@uva.nl, a.schrijver@uva.nl. The research leading to these results has received funding from the European Research Council under the European Union's Seventh Framework Programme (FP7/2007-2013) / ERC grant agreement №339109.

For n even it is not hard to see that $\Theta(C_n) = n/2$.

The Shannon capacity of C_7 is still unknown and its determination is a notorious open problem in extremal combinatorics [4, 7]. Many lower bounds have been given by explicit independent sets in some fixed power of C_7 [3, 12, 14], while the best known upper bound is $\Theta(C_7) \leq \vartheta(C_7) < 3.3177$. Here we give an independent set of size 367 in C_7^5, which yields $\Theta(C_7) \geq 367^{1/5} > 3.2578$. The best previously known lower bound on $\Theta(C_7)$ is $\Theta(C_7) \geq 350^{1/5} > 3.2271$, found by Mathew and Östergård [12]. They proved that $\alpha(C_7^5) \geq 350$ using stochastic search methods that utilize the symmetry of the problem. In [3], a construction is given of an independent set of size $7^3 = 343$ in C_7^5. The best known lower bound on $\alpha(C_7^4)$ is 108, by Vesel and Žerovnik [14]. See Table 1 for the currently best known bounds on $\alpha(C_7^d)$ for small d.

d	1	2	3	4	5
$\alpha(C_7^d)$	3	10^a	33^d	108^e–115^b	367^f–401^c

Table 1: Bounds on $\alpha(C_7^d)$. Key:
^{a} $\alpha(C_n^2) = \lfloor (n^2 - n)/4 \rfloor$ [3, Theorem 2]
^{b} $\alpha(C_n^d) \leq \alpha(C_n^{d-1})n/2$ [3, Lemma 2]
^{c} $\alpha(G^d) \leq \vartheta(G)^d$ by Lovász [11]
^{d} Baumert et al. [3]
^{e} Vesel and Žerovnik [14]
^{f} this paper, see the Appendix for the explicit independent set.

For comparison, $\alpha(C_7^3)^{1/3} = 33^{1/3} \approx 3.2075$, $\alpha(C_7^4)^{1/4} \geq 108^{1/4} \approx 3.2237$ and the previously best known lower bound on $\alpha(C_7^5)^{1/5}$ is $350^{1/5} \approx 3.2271$. Now we know that $\alpha(C_7^5) \geq 367 > 3.2578^5$.

The paper is organized as follows. In Section 2 we will examine the circular graphs $C_{k,n}$. We give a construction that yields independent sets in certain $C_{k,n}^d$, and we give an explicit description of an independent set S of size 382 in the graph $C_{108,382}^5$. This independent set does not translate directly to an independent set in C_7^5. However, in Section 3 we describe how one can obtain an independent set of size 367 in C_7^5 from S, by adapting S, removing vertices and adding new ones. This independent set is given explicitly in the Appendix.

2 Circular Graphs

For two integers a, b, let $[a, b]$ denote the set $\{a, a+1, \ldots, b\}$. For $k, n \in \mathbb{Z}$ with $n \geq 2k$, the *circular graph* $C_{k,n}$ is the graph with vertex set $\mathbb{Z}_n$, the cyclic group of order n, in which two distinct vertices are adjacent if and only if their distance (mod n) is strictly less than k. In other words, it is the *circulant graph* on $\mathbb{Z}_n$ with *generating set* $[1, k-1]$, which means that $V = \mathbb{Z}_n$ and $E = \{\{u, v\} \mid u - v \in [1, k-1]\}$. So $C_{2,n} = C_n$ and $C_{k,n}$ has vertex set $V(C_n) = \mathbb{Z}_n$. A closed formula for $\vartheta(C_{k,n})$, Lovász's upper bound on $\Theta(C_{k,n})$, is given in [2].

Note that by definition there is an edge between two distinct vertices x, y of $C_{k,n}^d$ if and only if there is an $i \in [1, d]$ such that $x_i - y_i$ (mod n) is either strictly smaller than k or strictly larger than $n - k$. For distinct u, v in $\mathbb{Z}_n^d$, define their *distance* to be the maximum over the distances of u_i and v_i (mod n), where i ranges from 1 to d. The *minimum distance* $d_{\min}(D)$ of a set $D \subseteq \mathbb{Z}_n^d$ is the minimum distance between any pair of distinct elements of D. (If $|D| = 1$, set $d_{\min}(D) = \infty$.) Then $d_{\min}(D) \geq k$ if and only if D is independent in $C_{k,n}^d$.

A homomorphism from a graph $G_1 = (V_1, E_1)$ to a graph $G_2 = (V_2, E_2)$ is a function $f : V_1 \to V_2$ such that if $ij \in E_1$ then $f(i)f(j) \in E_2$ (in particular, $f(i) \neq f(j)$). If there exists a homomorphism $f : G_1 \to G_2$ we write $G_1 \to G_2$. For any graph G, we write $\overline{G}$ for the complement of G. If $\overline{G} \to \overline{H}$, then $\alpha(G) \leq \alpha(H)$ and $\Theta(G) \leq \Theta(H)$. The circular graphs have the property that $\overline{C_{k',n'}} \to \overline{C_{k,n}}$ if and only if $k'/n' \leq k/n$ [5]. So if $k'/n' \leq k/n$, then $\alpha(C_{k',n'}^d) \leq \alpha(C_{k,n}^d)$ (for any d) and $\Theta(C_{k',n'}) \leq \Theta(C_{k,n})$. Moreover, $\alpha(C_{k,n}^d)$ and $\Theta(C_{k,n})$ only depend on the fraction n/k.

An independent set in $C^d_{k,n}$ gives an independent set in $C^d_{\lceil 2n/k \rceil}$, since $\overline{C_{k,n}} \to \overline{C_{2,\lceil 2n/k \rceil}}$. Explicitly, consider the elements of $\mathbb{Z}_n$ as integers between 0 and $n-1$ and replace each element i by $\lfloor 2i/k \rfloor$, and consider the outcome as an element of $\mathbb{Z}_{\lceil 2n/k \rceil}$. This gives indeed a homomorphism $\overline{C_{k,n}} \to \overline{C_{2,\lceil 2n/k \rceil}}$ as the image of any two elements with distance at least k has distance at least 2.

First, we will give an independent set of size 382 in $C^5_{108,382}$. As $382/108 > 7/2$ this does not directly give an independent set in $C^5_{2,7}$. However, in Section 3 we try to adapt the independent set, remove some words and add as many new words as possible to obtain a large independent set in C^5_7.

Proposition 2.1. *The set* $S := \{t \cdot (1, 7, 7^2, 7^3, 7^4) \mid t \in \mathbb{Z}_{382}\} \subseteq \mathbb{Z}^5_{382}$ *is independent in* $C^5_{108,382}$.

Proof. If $x, y \in S$ then also $x - y \in S$. So it suffices to check that for all nonzero $x \in S$:

$$\exists\ i \in [1, 5] \text{ such that } x_i \in [108, 274]. \tag{3}$$

Let $x = t \cdot (1, 7, 7^2, 7^3, 7^4) \in S$ be arbitrary, with $0 \neq t \in \mathbb{Z}_{382}$. For $t \in [108, 274]$ clearly (3) holds with $i = 1$ (as then $x_i = t \in [108, 274]$). Also we have $[275, 381] = -[1, 107]$, so it suffices to verify (3) for $t \in [1, 107]$. Note that for $t \in [16, 39]$ one has $108 \leq 7t \leq 274$, so (3) is satisfied with $i = 2$. Also note that $69 \cdot 7 \equiv 101 \pmod{382}$. So for $t \in [70, 93]$ one has $7t \equiv 101 + 7(t - 69) \pmod{382} \in [108, 274]$, i.e., (3) is satisfied with $i = 2$. For the remaining $t \in [1, 107]$, please take a glance at Table 2. In each row, in each of the three subtables, there is at least one entry in $[108, 274]$. This completes the proof. $\square$

1	7	49	343	109
2	14	98	304	218
3	21	147	265	327
4	28	196	226	54
5	35	245	187	163
6	42	294	148	272
7	49	343	109	381
8	56	10	70	108
9	63	59	31	217
10	70	108	374	326
11	77	157	335	53
12	84	206	296	162
13	91	255	257	271
14	98	304	218	380
15	105	353	179	107
40	280	50	350	158
41	287	99	311	267
42	294	148	272	376
43	301	197	233	103
44	308	246	194	212

45	315	295	155	321
46	322	344	116	48
47	329	11	77	157
48	336	60	38	266
49	343	109	381	375
50	350	158	342	102
51	357	207	303	211
52	364	256	264	320
53	371	305	225	47
54	378	354	186	156
55	3	21	147	265
56	10	70	108	374
57	17	119	69	101
58	24	168	30	210
59	31	217	373	319
60	38	266	334	46
61	45	315	295	155
62	52	364	256	264
63	59	31	217	373
64	66	80	178	100

65	73	129	139	209
66	80	178	100	318
67	87	227	61	45
68	94	276	22	154
69	101	325	365	263
94	276	22	154	314
95	283	71	115	41
96	290	120	76	150
97	297	169	37	259
98	304	218	380	368
99	311	267	341	95
100	318	316	302	204
101	325	365	263	313
102	332	32	224	40
103	339	81	185	149
104	346	130	146	258
105	353	179	107	367
106	360	228	68	94
107	367	277	29	203

Table 2: Part of the verification that S is independent in $C^5_{108,382}$.

The authors found the above independent set when looking for answers to the following question.

$$\text{For } n, d, q, \text{ what is the minimum distance } k(n, d, q) \text{ of } \{t \cdot (1, q, \ldots, q^{d-1}) \mid t \in \mathbb{Z}_n\} \subseteq \mathbb{Z}^d_n\,? \tag{4}$$

The independent set from Proposition 2.1 was found by computer (with $n \geq 350$ and $d = 5$ such that $n/k(n, d, q)$ is close to $7/2$). Question (4) seems not easy to solve in general.

3 Description of the method

Here we describe how to use the independent set from Proposition 2.1 to find an independent set of size 367 in C^5_7. The procedure is as follows.

(i) Start with the independent set S in $C^5_{108,382}$ from Proposition 2.1.

(ii) Add the word $(40, 123, 40, 123, 40) \bmod 382$ to each word in S.

(iii) Replace each letter i, which we now consider to be an integer between 0 and 381 and not anymore an element in $\mathbb{Z}_{382}$, in each word from S by $\lfloor i/54.5 \rfloor$. Now we have a set of words S' with only symbols in $[0, 6]$ in it, which we consider as elements of $\mathbb{Z}_7$.

(iv) Remove each word $u \in S'$ for which there is a $v \in S'$ such that $uv \in E(C_7^5)$ from S', i.e., we remove u if there is a $v \in S'$ with $v \neq u$ such that $u_i - v_i \in \{0, 1, 6\}$ for all $i \in [1, 5]$. We denote the set of words which are not removed from S' by this procedure by M. The computer finds $|M| = 327$. Note that M is independent in C_7^5.

(v) Find the best possible extension of M to a larger independent set in C_7^5. To do this, consider the subgraph G of C_7^5 induced by the words x in $\mathbb{Z}_7^5$ with the property that $M \cup \{x\}$ is independent in C_7^5. This graph is not large, in this case it has 71 vertices and 85 edges, so a computer finds a maximum size independent set I in G quickly. The computer finds $|I| = \alpha(G) = 40$, so we can add 40 words to M. Write $R := M \cup I$. Then $|R| = 327+40 = 367$ and R is independent in C_7^5.

The maximum size independent set I in the graph G in (v) was found using Gurobi [8]. In steps (ii) and (iii), many possibilities for adding a constant word and for the division factor were tried, but no independent set of size 368 or larger was found. Also, the independent set R of size 367 did not seem to be easily extendable. A local search was performed, showing that there exists no triple of words from R such that if one removes these three words from R, four words can be added to obtain an independent set of size 368 in C_7^5.

Remark 3.1. One other new bound on $\alpha(C_n^d)$ was obtained (for $n \leq 15$ and $d \leq 5$) using independent sets of the form from (4). With $n = 4009$, $d = 5$ and $q = 27$, we found $k(n, d, q) = 729$. As $n/(k(n, d, q)) = 4009/729 < 11/2$, this directly yields the new lower bound $\alpha(C_{11}^5) \geq 4009$. The previously best known lower bound is $\alpha(C_{11}^5) \geq 3996$ from [12]. However, the new lower bound on $\alpha(C_{11}^5)$ does not imply a new lower bound on $\Theta(C_{11})$. It is known that $\Theta(C_{11}) \geq \alpha(C_{11}^3)^{1/3} = 148^{1/3} > 5.2895$ (cf. [3]), which is larger than $4009^{1/5}$.

Appendix: explicit code

The following 367 words form an independent set in C_7^5, which proves the new bound $\Theta(C_7) \geq 367^{1/5} > 3.2578$. It is the set R from Section 3.

```
02020,02112,02204,02306,02461,02553,03645,03040,03032,03124,03226,03311,03403,14144,14231,14323,14415,14510,15602,15064,15166,15251,15343,
15430,15522,16614,16016,16101,16263,16355,16450,16542,10636,10021,10113,10205,10300,10462,10554,11656,11041,11033,11125,11220,11312,11404,
11506,12661,12053,12145,12240,12232,12324,12426,12511,13603,13065,13160,13252,13344,13446,13431,24010,24102,24264,24366,24451,24543,25630,
25022,25114,25216,25301,25463,25555,26650,26042,26034,26136,26221,26313,26405,26500,20662,20054,20156,20241,20233,20325,20420,20512,21604,
21006,21161,21253,21345,21440,21432,22626,22011,22103,22265,22360,22452,22544,23631,23023,23115,23210,23302,23464,23566,34130,34222,34314,
34416,34501,35663,35055,35150,35242,35234,35336,35421,35513,36605,36000,36162,36254,36356,36441,36433,30620,30012,30104,30206,30361,30453,
30545,31632,31024,31126,31211,31303,31465,31560,32652,32044,32131,32223,32315,32410,32502,33664,33066,33151,33243,33235,33330,33422,44616,
44001,44163,44255,44350,44442,44434,44536,45621,45013,45105,45200,45362,45454,45556,46633,46025,46120,46212,46304,46406,46561,40653,40045,
40132,40224,40326,40411,40503,41665,41060,41152,41244,41331,41423,41515,42610,42002,42164,42266,42351,42443,42435,43622,43014,43116,43201,
43363,43455,43550,54634,54036,54121,54213,54305,54400,54562,55654,55056,55141,55133,55225,55320,55412,55504,56606,56061,56153,56245,56332,
56424,56526,50611,50003,50165,50260,50352,50444,51623,51015,51110,51202,51364,51551,52643,52635,52030,52122,52214,53655,53134,64332,64424,
64526,65611,65003,65260,65352,65444,65546,66623,66110,66202,66364,66466,66551,60643,60645,60030,60122,60214,60316,60401,60563,61050,61142,
61134,61236,61321,61413,62600,62062,62154,62256,62341,62333,62520,63612,63004,63106,63261,63353,63445,63540,64532,04026,04111,04203,04460,
04552,05644,05031,05123,05310,05402,05564,06666,06051,06143,06230,06322,06414,06516,00601,00063,00155,00250,00342,00334,00436,01613,01100,
01262,01354,01456,01541,02625,00521,01005,02533,03565,04052,04365,04624,04660,05046,05225,10534,14246,15435,22524,24615,24651,32046,34035,
34043,36525,40040,41246,42530,43514,45641,50531,51456,52400,52563,53050,53142,53320,53412,56340,61505,62425,64154,64340,65105,66025.
```

Acknowledgements

The authors want to thank Bart Litjens, Bart Sevenster, Jeroen Zuiddam and the two anonymous referees for very useful comments.

References

[1] N. Alon, The Shannon capacity of a union, *Combinatorica*, 18 (1998), 301–310.

[2] C. Bachoc, A. Pêcher, A. Thiéry, On the theta number of powers of cycle graphs, *Combinatorica*, 33 (2013), 297–317.

[3] L. Baumert, R. McEliece, E. Rodemich, H. Rumsey, R. Stanley, H. Taylor, A combinatorial packing problem, *Computers in Algebra and Number Theory*, American Mathematical Society, Providence, RI (1971), 97–108.

[4] T. Bohman, A limit theorem for the Shannon capacities of odd cycles I, *Proceedings of the American Mathematical Society*, 131 (2003), 3559–3569.

[5] J.A. Bondy, P. Hell, A note on the star chromatic number, *Journal of Graph Theory*, 14 (1990), 479–482.

[6] M. Fekete, Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten, *Mathematische Zeitschrift*, 17 (1923), 228–249.

[7] C.D. Godsil, Problems in algebraic combinatorics, *Electronic Journal of Combinatorics*, 2 (1995), 1–20.

[8] Gurobi Optimization, LLC, *Gurobi Optimizer Reference Manual*, 2018, `http://www.gurobi.com`.

[9] W.H. Haemers, On some problems of Lovász concerning the Shannon capacity of a graph, *IEEE Transactions on Information Theory*, 25 (1979), 231–232.

[10] M. Jurkiewicz, M. Kubale, K. Turowski, Some lower bounds on the Shannon capacity, *Journal of Applied Computer Science*, 22 (2014), 31–42.

[11] L. Lovász, On the Shannon capacity of a graph, *IEEE Transactions on Information Theory*, 25 (1973), 1–7.

[12] K.A. Mathew, P.R.J. Östergård, New lower bounds for the Shannon capacity of odd cycles, *Designs, Codes and Cryptography*, 84 (2017), 13–22.

[13] C.E. Shannon, The zero-error capacity of a noisy channel, *IRE Transactions on Information Theory*, 2 (1956), 8–19.

[14] A. Vesel, J. Žerovnik, Improved lower bound on the Shannon capacity of C_7, *Information Processing Letters*, 81 (2002), 277–282.

[15] J. Zuiddam, The asymptotic spectrum of graphs and the Shannon capacity, `arXiv` 1807.00169 (2018).