New Linear Codes from Constacyclic Codes

John M. Murphree (Nuh Aydin, advisor)
Department of Mathematics, Kenyon College, Gambier, OH

Kenyon College

Abstract

One of the main challenges of coding theory is to construct linear codes with the best possible parameters. Various algebraic and combinatorial methods along with computer searches are used to construct codes with better parameters. Given the computational complexity of determining the minimum distance of a code, exhaustive searches are not feasible for all but small parameter sets. Therefore, we chose to focus on the class of constacyclic codes, as we can exhaustively generate constacyclic codes over small finite fields of order up to 9 to create a database of best constacyclic codes. We will then use this database as a building block for a search algorithm for new quasi-twisted codes. We used a search strategy that is comprehensive, i.e., it computes every constacyclic code for a given length and shift constant, and it avoids redundantly examining constacyclic codes that are equivalent to either cyclic codes we have already searched, or other constacyclic codes. Using this method, we have constructed 75 (16 constacyclic + 59 standard constructions) new codes. This is a surprising amount, as constacyclic codes have already been extensively researched.

Linear Codes

Definition *A linear code of length* n *and rank* k *is a linear subspace* C *with dimension* k *of the vector space* F^n_q *where* F_q *is the finite field with q elements.*

Some Applications

Linear codes are often used in communicating electronic data. For example, a BCH linear code is used to encode information to a CD. Similarly, barcode scanners utilize linear codes

Constacyclic Codes

Definition *Let a be a non-zero constant in* $\mathbf{F_q}$ *. A linear code C is called constacyclic if it is closed under the constacyclic shift, i.e. whenever* $(c_0 , c_1 , \dots , c_{n-1}) \epsilon C$ *then* $(ac_{n-1} , c_0 , c_1 , \dots, c_{n-2}) \epsilon C$ *as well.*

Note, cyclic codes are a specific case of constacyclic code, the case where a=1.

Generating Constacyclic Codes

There is a one to one correspondence between the divisors of x^n-a, where n is the length of a code and a is the shift constant, and codes of length n. That is, for each possible polynomial, g(x), that is created as a product of irreducible factors of x^n-a, there exists a constacyclic code generated by g(x).

VerifyMinimumDistanceLowerBound()

Another addition to make our search code more efficient was the VerifyMinimumDistanceLowerBound() function. Presented A code, C, and a value, d (the current best stored minimum distance value) are passed to this function. It is run until d is found to be a lower bound of the minimum distance of C, or returns false if it is not. This function will often save computational time, but this is not guaranteed.

Parameters

One of the novelties of our search code that was influential in allowing us to exhaustively search constacyclic codes was setting parameters on the time-consuming function used to calculate minimum distance. To ensure that the MinimumDistance() function did not take up too much time, we used the MaximumTime parameter to restrict the execution time of this function to two minutes. After this period, the calculation is aborted, the generator polynomial of the code is displayed, and a new code calculation is begun.

New Codes

q	n	$g(x)$ or $h(x)$	k	d	a
3	182	$h(x) = x^{22} + x^{21} + 2x^{20} + 2x^{19} + 2x^{17} + x^{13} + 2x^{11} + 2x^9 + x^8 + x^7 + x^4 + x^3 + 2x + 2$	22	86	1
3	182	$h(x) = x^{24} + x^{23} + x^{22} + x^{21} + 2x^{19} + 2x^{18} + 2x^{17} + x^{16} + 2x^{14} + 2x^{13} + 2x^{10} + 2x^8 + x^7 + x^6 + 2x^5 + x^3 + 2$	24	84	1
3	182	$h(x) = x^{25} + x^{24} + x^{23} + x^{21} + 2x^{19} + x^{18} + x^{17} + 2x^{15} + x^{13} + 2x^{11} + x^{10} + 2x^9 + 2x^8 + 2x^7 + x^6 + 2x^5 + 2x^3 + x + 2$	25	83	1
3	205	$h(x) = x^{17}+2x^{15}+2x^{14}+2x^{13}+x^{10}+2x^9+2x^8+2x^7+x^4+2x^3+2x^2+2$	17	109	1
3	70	$x^{22}+x^{20}+2x^{19}+x^{18}+x^{16}+2x^{15}+x^{14}+2x^{13}+x^{11}+x^9+2x^8+x^5+2x^2+1$	48	10	2
3	146	$h(x) = x^{24} + x^{23} + 2x^{21} + 2x^{20} + 2x^{16} + 2x^{15} + x^{13} + x^{12} + 2x^{11} + x^9 + 2x^8 + 2x^4 + x^3 + 2x + 1$	24	66	2
3	146	$h(x) = x^{26} + x^{25} + x^{24} + 2x^{22} + 2x^{21} + 2x^{20} + 2x^{18} + 2x^{17} + 2x^{16} + x^{14} + x^{12} + 2x^{10} + x^9 + 2x^8 + 2x^6 + x^5 + 2x^4 + x^2 + 2x + 1$	26	62	2
5	78	$x^{26} + 4x^{25} + 2x^{24} + 2x^{22} + x^{21} + 3x^{19} + x^{17} + 4x^{16} + 2x^{15} + 2x^{14} + x^{13} + 3x^{12} + 3x^{10} + 3x^9 + 4x^8 + 3x^6 + 4x^5 + 3x^4 + 2x^3 + x + 2$	52	13	2
5	78	$x^{24} + 4x^{23} + 4x^{22} + x^{21} + x^{20} + x^{19} + 4x^{17} + 4x^{16} + 3x^{15} + 4x^{14} + x^{13} + 4x^{12} + x^{10} + x^9 + x^8 + 4x^7 + 3x^6 + 3x^4 + 4x^3 + 2x^2 + 1$	54	12	2
5	78	$x^{22} + x^{21} + 3x^{20} + 2x^{19} + 4x^{18} + 4x^{17} + x^{16} + 4x^{15} + 3x^{14} + x^{11} + x^{10} + x^8 + 4x^6 + 2x^5 + x^4 + 4x^3 + 4x^2 + 4x + 3$	56	11	2
5	78	$x^{18} + 4x^{17} + 4x^{15} + x^14 + 4x^{12} + 2x^{11} + 4x^{10} + 4x^9 + 4x^8 + 3x^7 + 3x^6 + 4x^5 + 2x^4 + 2x^3 + 4x^2 + 2$	60	9	2
5	78	$x^{10} + x^9 + 3x^8 + 2x^7 + 4x^6 + 3x^5 + 2x^4 + x^3 + 2x^2 + 2$	68	6	2
7	48	$h(x) = x^{17} + 3x^{16} + 3x^{15} + 6x^{14} + 6x^{13} + 5x^{12} + x^{11} + 5x^{10} + 3x^8 + 2x^7 + 3x^6 + 2x^5 + 6x^4 + 3x^3 + 5x^2 + 2$	17	22	1
7	57	$x^{21} + 2x^{20} + 4x^{19} + 2x^{18} + 6x^{17} + x^{16} + 5x^{14} + 6x^{13} + 6x^{11} + 3x^9 + 6x^8 + 4x^6 + 4x^5 + 6x^4 + 5x + 4$	36	13	3
7	57	$x^{24} + 4x^{22} + 2x^{21} + 5x^{20} + 5x^{19} + 2x^{18} + x^{17} + 2x^{16} + x^{15} + 6x^{14} + x^{13} + 2x^{12} + 2x^{11} + 6x^{10} + x^9 + 4x^7 + 4x^6 + 3x^4 + x^3 + 3x^2 + 2$	33	15	3
9	58	$x^{28} + \alpha^6x^{27} + \alpha^2x^{26} + \alpha x^{25} + \alpha^7x^{23} + \alpha^6x^{21} + x^{20} + 2x^{18} + 2x^{17} + \alpha^5x^{16} + \alpha^7x^{15} + \alpha^2x^{14} + x^{13} + \alpha^7x^{12} + \alpha^7x^{11} + x^{10} + \alpha^6x^8 + \alpha^5x^7 + x^5 + 2x^3 + \alpha^6x^2 + \alpha^3x + \alpha^6$	30	18	α

In addition to these 16 new codes, we have constructed 59 codes through the means of the standard constructions -- extending, shortening, and puncturing. It was surprising for us to find so many constacyclic codes, as they have already been frequently searched.

Proposition

Let α , β ϵ $\mathbf{F_q}$ *such that |α| = |β|, where |α| denotes the order of α in the multiplicative group of non-zero elements of* $\mathbf{F_q}$ *. Then α has an nth root in* $\mathbf{F_q}$ *if and only if β does.*

We offer this proposition, which we introduced to aid our comprehensive search of constacyclic codes. To understand its significance in our method, we first recall the following Lemma [1], using the polynomial x^n-a where n is the length of the code and a is the shift constant:

Lemma *If* $\mathbf{F_q}$ *contains an nth root δ of a, then a constacyclic code of length n is equivalent to a cyclic code of length n.*

Furthermore, we know exactly when an element a ϵ $\mathbf{F_q}$ has an nth root in $\mathbf{F_q}$:

Lemma 2 [2] *Let* $a=\alpha^i$ *where α is a primitive element of* $\mathbf{F_q}$*. Then the equation* $x^n=a$ *has a solution in* $\mathbf{F_q}$ *if and only if gcd(n,q-1)|i.*

Using these two lemmas and our proposition, we know that a constacyclic code with shift constant *a* and a constacyclic code with shift constant *b* will be equivalent if *a* and *b* have the same order. So, we only needed to search the shift constants outlined in the table below.

q	$a \neq 0, 1$	n
3	2	all $n \ni 2\|n$
4	any constant in field	all $n \ni 3\|n$
5	2	all $n \ni 2\|n$
	4	all $n \ni 4\|n$
7	2	all $n \ni 3\|n$
	3	all $n \ni 2\|n$ or $n \ni 3\|n$
	6	all $n \ni 2\|n$
8	any constant in field	all $n \ni 7\|n$
9	α	all $n \ni 2\|n$
	α^2	all $n \ni 4\|n$
	α^4	all $n \ni 8\|n$

Acknowledgements

I would like to thank Kenyon College Summer Science and Professor Aydin for aiding me in my research, the Young Mathematicians Conference for giving me the opportunity to present my results, and my family for the support they've always offered.

References

1. N. Aydin, I. Siap and D. Ray-Chaudhuri "The structure of 1-generator quasi-twisted codes and new linear codes", Designs Codes and Cryptography, Vol. 23, No.3, pp. 313-326, December 2001.
2. S. Roman, *Coding and Information Theory, Graduate Texts in Mathematics* 134 (Springer-Verlag, 1992).