

Conjectures on the Size of Constellations Constructed from Direct Sums of PSK Kernels

Matthew G. Parker**

Department of Informatics, University of Bergen, N-5020 Bergen, Norway,
matthew@ii.uib.no

Abstract. A general equation is given for the size of complex constellations constructed from the direct sum of PSK-like constellation primitives. The equation uses a generating function whose numerator is a power of a 'coordination polynomial'. Conjectures are also given as to the form and value of these coordination polynomials for various PSK. The study has relevance to error-coding, polynomial residue number theory, and the analysis of random walks.

1 Introduction

Communications systems often transmit data by modulating using Binary or Quaternary Phase Shift Keyed (BPSK or QPSK) or Quadrature Amplitude Modulated (QAM) constellations in the complex plane. But larger constellations can be more bandwidth-efficient and lead to efficient hardware implementation of complex arithmetic and algorithms [1,2]. This paper considers the problem of finding the size of constellations constructed from direct sums of {PSK plus the origin}, referred to here as 'PSK \oplus ' constellations. These constellations form lattices for 1,2,3, or 6 PSK primitives, but for any other PSK \oplus there will be residue 'folding' making the determination of constellation size more complicated. This problem can be recast, for m PSK \oplus , as finding an expression for the number of non-identical polynomial residues resulting from the reduction, mod $\Phi_m(x)$, of polynomials in x of Coefficient Weight $\leq n$, (for some positive integer, n), and degree $< m$, where $\Phi_m(x)$ is the m^{th} cyclotomic polynomial in x . Although residue folding is, for many applications, undesirable, it is hoped that an algebraic understanding of PSK \oplus will help in the construction of constellations more suited to communications systems which use PSK \oplus as building blocks. Also, from an algebraic point of view, it is useful to be able to enumerate the residues of polynomials, mod $\Phi_m(x)$. The theorem and conjectures to be presented here are based on computational results. During the course of the work integer sequences, relating to the 8PSK \oplus and 16PSK \oplus constellations, were entered into Sloane's On-Line Encyclopedia of Integer Sequences [3] and were found to refer, in particular, to the paper by Conway and Sloane on Low Dimensional Lattices [4] which, in turn, references work by O'Keefe [5] and others [6].

** This work was funded by NFR Project Number 119390/431

Their results have applications to crystallography, and use generating functions which require the specification of a 'Coordination Sequence'. This paper conjectures a general solution to a related problem, although a general form for the Coordination Sequence (Polynomial) has yet to be found. The results could be used to help extend the scope of error coding strategies such as [7, 8], and may also be useful for the development of 'Random Walk' statistics.

2 Statement of the Problem

Define $m\text{PSK}+$ as the set of $m + 1$ points in the complex plane given by,

$$m\text{PSK}+ = \{0, 1, w, w^2, \dots, w^{m-1}\}$$

where $w = e^{\frac{2\pi i}{m}}$, and $i^2 = -1$. Define $m\text{PSK} \oplus n$ as the direct sum of n copies of $m\text{PSK}+$, given by,

$$m\text{PSK} \oplus n = \sum_{k=0}^{n-1} \{0, 1, w, w^2, \dots, w^{m-1}\}$$

We wish to find a formula for d_n as n varies over the positive integers, where d_n is the number of non-identical points in $m\text{PSK} \oplus n$, given by,

$$d_n = \left| \sum_{k=0}^{n-1} \{0, 1, w, w^2, \dots, w^{m-1}\} \right|$$

For instance, let $m = 4$. The kernel constellation is $\{0, 1, w, w^2, w^3\}$, where $w = e^{\frac{2\pi i}{4}}$, and,

$$d_2 = \left| \sum_{k=0}^1 \{0, 1, w, w^2, w^3\} \right| = |\{0, \pm 1, \pm w, \pm 1 \pm w, \pm 1 \mp w, \pm 2, \pm 2w\}| = 13$$

As another example, for $m = 6$ and $n = 2$,

$$d_2 = |\{0, \pm 1, \pm w, \pm w^2, \pm 2, \pm 2w, \pm 2w^2, \pm 1 \pm w, \pm 1 \mp w^2, \pm w \mp w^2\}| = 19$$

An algebraic description of the same problem is as follows.

Definition 1 *The 'Coefficient Weight', (cw), of a polynomial, $f(x)$, is the sum of its coefficient values. In other words $cw(f(x)) = f(1)$.*

Let $g(x) = \sum_i g_i x^i$. Let,

$$\mathbf{G}_{\mathbf{m}, \mathbf{n}} = \{g(x) \mid 0 \leq \deg(g(x)) < m, g_i \geq 0 \ \forall i, 0 \leq cw(g(x)) \leq n\}$$

where $\deg(a(x))$ is the degree of $a(x)$. Let $x = e^{\frac{2\pi i}{m}}$, where $i^2 = -1$. Then,

$$m\text{PSK} \oplus n = \{h(x) \mid h(x) = \langle g(x) \rangle_{\Phi_m(x)}, \forall g(x) \in \mathbf{G}_{\mathbf{m}, \mathbf{n}}\}$$

where $\langle a \rangle_b$ is the residue of a mod b , and $\Phi_m(x)$ is the m^{th} cyclotomic polynomial. Therefore,

$$d_n = |m\text{PSK} \oplus n|$$

as before.

3 Computational Results

Tables 1 and 2 show some computed values of d_n for various n and m . The number of Euclidean distances, D , refers to the size of the set of values for the absolute (straight-line) distance from each point in $m\text{PSK} \oplus n$ to the origin. The figures for D are not discussed further in this paper, but are included here for the reader's interest.

Table 1. Constellation and Euclidean Distance Enumerations for Various $m\text{PSK} \oplus n$
 d_n -No of points in constellation. D -No of Euclidean distances.

n	1		2		3		4		5		6		7		8		9		10	
m	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D	d_n	D
3	4	2	10	3	19	5	31	7	46	9	64	12	85	15	109	18	136	22	166	26
4	5	2	13	4	25	6	41	9	61	12	85	16	113	19	145	24				
5	6	2	21	5	56	8	126	17												
6	7	2	19	4	37	6	61	9	91	12	127	16	169	20						
7	8	2	36	6	120	14	330	30												
8	9	2	41	6	129	13	321	29	681	53	1289	96	2241	3649	5641	8361				
9	10	2	55	6	217	17	685	46	1837	99										
10	11	2	61	7	211	17	551	38	1201	72										
12	13	2	73	7	253	16	661	38	1441	72										
14	15	2	113	9	575	29	2171	96												
15	16	2	136	9	811	33	3751	132	14176	440										
16	17	2	145	10	833	35														
18	19	2	163	10	865	33	3313	114												
20	21	2	221	12	1521	46														
21	22	2	253	12	2017	59	12496	322	63946	1396										
22	23	2	265	13	2047	59	11969	310												
24	25	2	289	13	2089	54	10825	258												
25	26	2	351	15	3276	78														
27	28	2	406	15	4051	89	31213	4296												
30	31	2	451	16	3901	81	22831	425												
33	34	2	595	18	7129	125	65671	1072												
35	36	2	666	20	8436	138														
36	37	2	649	19	7237	118														
40	41	2	841	22	11441	161														
45	46	2	1081	24	17281	213														
48	49	2	1153	25																
49	50	2	1275	27																
50	51	2	1301	27	22051	246														
54	55	2	1459	28	24949	258														
60	61	2	1801	31	33901	310														
75	76	2	2926	39																
90	91	2	4051	46																

And here are a few more partial results for the case $m = 8$.

Table 2. Constellation Enumerations for More $8\text{PSK} \oplus n$

n	11	12	13	14	15
m	d_n	d_n	d_n	d_n	d_n
8	11969	16641	22569	29961	39041

4 Some Conjectures

We shall form a generating function for the sequences, d_n , where d_n is different for every m . Thus define $d_m(x) = \sum_{n=0}^{\infty} d_n x^n$. The following conjecture satisfies all numerical results quoted above,

Conjecture 1

$$d_m(x) = \frac{c_h(x)^{\frac{m}{h}}}{(1-x)^{\phi(m)+1}}$$

where ϕ is Euler's Totient Function, h is the square free part of m , and $c_h(x)$ is referred to as the h^{th} coordination polynomial. $c_h(x)$ is palindromic and $\deg(c_h(x)) = \phi(h)$.

The above conjecture omits to specify exactly the form of $c_h(x)$. This is an area of further research. However the following theorem determines $c_h(x)$ where h is a prime, and two following conjectures satisfy the computational results for $h = 2p$, p an odd prime, and $h = 15$, respectively,

Theorem 1

$$c_p(x) = \Phi_p(x), \quad p \text{ prime}$$

Theorem 1 was conjectured by the author based on numerical computation. A proof was found by T.Kløve and it is given in Appendix A.

Conjecture 2

$$c_{2p}(x) = \sum_{k=0}^{\frac{p-3}{2}} x^k + x^{p-1-k} \sum_{i=0}^k \binom{p}{i} + x^{\frac{p-1}{2}} \sum_{i=0}^{\frac{p-1}{2}} \binom{p}{i}, \quad p \text{ an odd prime}$$

Conjecture 3

$$c_{15}(x) = (1 + x^8) + 7(x + x^7) + 28(x^2 + x^6) + 79(x^3 + x^5) + 130x^4$$

The following observation was also made,

Conjecture 4

$$m \mid \left(\frac{m^{n+1} - 1}{m - 1} - d_n \right)$$

From the computational results values of $c_h(x)$ have also been partially ascertained for various h as shown in Table 3.

All preceding coordination polynomials were computed from the d_n sequences using the following strategy. For instance, for $m = 6$ the d_n sequence is computed to be 1,7,19,37,61,91,127,169,.... Thus $d_6(x) = 1+7x+19x^2+37x^3+61x^4+91x^5+127x^6+169x^7+\dots$. Note that $\phi(6) + 1 = 3$ so, from Conjecture 1, we multiply $d_6(x)$ (truncated to degree 7) by $(1-x)^3$ to get $c'_6(x) = e(x) + x^2 + 4x + 1$, where $e(x)$ is some error term due to having truncated $d_6(x)$ to degree 7. In this case $e(x) = -217x^8 + 380x^9 - 169x^{10}$, which is evidently an error term so $c_6(x) = x^2 + 4x + 1$. The same strategy can be used to compute $c_h(x)$ for all d_n sequences in the table, and hence arrive at the preceding Conjectures 2 - 3 on the form of $c_h(x)$.

Lemma 1 *We have*

$$\sum_{n=0}^{\infty} p_r(n)x^n = \frac{1}{(1-x)^r} \quad \text{and} \quad \sum_{n=r-1}^{\infty} p_r(n-(r-1))x^n = \frac{x^{r-1}}{(1-x)^r}$$

Proof of Lemma 1: These are standard results from the theory of partitions:

$$\sum_{n=0}^{\infty} p_r(n)x^n = (1+x+x^2+x^3+\dots)^r = \frac{1}{(1-x)^r}$$

and

$$\sum_{n=r-1}^{\infty} p_r(n-(r-1))x^n = x^{r-1} \sum_{n=r-1}^{\infty} p_r(n-(r-1))x^{n-(r-1)} = \frac{x^{r-1}}{(1-x)^r}. \quad \blacksquare$$

Lemma 2 *Let m be an odd prime. Then $d_n = p_{m+1}(n) - p_{m+1}(n-m)$.*

Proof of Lemma 2: d_n counts the number of distinct sums

$$a_1w + a_2w^2 + \dots + a_mw^m + a_{m+1} \cdot 0 \quad (1)$$

where $a_i \geq 0$ for $i = 1, 2, \dots, m+1$ and $a_1 + a_2 + \dots + a_{m+1} = n$. Noting that $w + w^2 + \dots + w^m = 0$ we get d_n by counting all sums (1), this number is $p_{m+1}(n)$, and subtracting the number of sums where $a_i \geq 1$ for $i = 1, 2, \dots, m$, this number is $p_{m+1}(n-m)$ (as explained above). \blacksquare

Theorem 1 now follows from the two lemmas:

$$\sum_{n=0}^{\infty} d_n x^n = \sum_{n=0}^{\infty} p_{m+1}(n)x^n - \sum_{n=0}^{\infty} p_{m+1}(n-m)x^n = \frac{1-x^m}{(1-x)^{m+1}} = \frac{\Phi_m(x)}{(1-x)^m}$$

since $\Phi_m(x) = x^m + x^{m-1} + \dots + 1$. \blacksquare

8 Appendix B - A General Strategy for Computing the Size of $\text{PSK} \oplus$ Constellations

Here a technique is proposed for the fast computation of the coefficients of $d_m(x)$ in the general case. Hopefully this may lead to a general proof of the conjectures of this paper, and a fast way to construct $c_h(x)$ in the general case, at least for m up to some large value. The technique will be illustrated by looking at the case where $m = 6$. Note that $\Phi_6(x) = x^2 - x + 1$. The steps of the technique are the following subsection headings.

8.1 Find all Forbidden Binary Patterns

$\Phi_6(x)$ implies the following polynomial equivalences:

$$x^2 + 1 = x \quad \text{pattern is } 101000$$

$$x^3 + 1 = 0 \quad \text{pattern is 100100}$$

These are the two **binary** patterns (polynomials) which are 'forbidden' for $m = 6$. The forbidden polynomials are the set of polynomials which are equivalent, mod $\Phi_m(x)$, to polynomials of lower hamming weight. Note that, for example, $x^2 - x + 1$ is not included as a 'forbidden' polynomial as it includes the polynomial $x^2 + 1$ as a sub-polynomial. In general, for $m = 2p$, p prime, there are only two forbidden polynomials, namely, $x^{p-1} + x^{p-3} + x^{p-5} + \dots + x^2 + 1$, and, $x^p + 1$. More generally, for large, composite m , there may be non-binary forbidden polynomials.

8.2 Enumerate all Length m Binary Words Which Avoid the Forbidden Patterns

For $m = 6$, and for Hamming Weights (hw) 0-6 we have the following cyclically distinct **binary** strings which avoid the forbidden patterns or any cyclic shift of the forbidden patterns.

hw = 0	000000
hw = 1	100000
hw = 2	110000
hw = 3	none
hw = 4	none
hw = 5	none
hw = 6	none

Each string of non-zero Hamming Weight has cyclic shift order 6. We will refer to the set of length m strings which avoid the forbidden patterns as the 'foundation' polynomials. These 'foundation' polynomials form the set \mathbf{E} . For $m = 6$ $|\mathbf{E}| = 3$. We will define there to be $e_{\text{hw},m}$ cyclically distinct length m binary words in \mathbf{E} , $0 \leq \text{hw} \leq m$. For $m = 6$, $e_{0,6} = 1$, $e_{1,6} = 1$, $e_{2,6} = 1$, $e_{3,6} = 0$, $e_{4,6} = 0$, $e_{5,6} = 0$, $e_{6,6} = 0$. Note that $e_{0,m} = 1 \forall m$.

8.3 Use Each Member of \mathbf{E} as a 'Foundation' for Building All Length m Inequivalent Polynomials of Coefficient Weight n , mod $\Phi_m(x)$

The '1' positions of the 'foundation' polynomials of \mathbf{E} mark the positions where we are allowed to add 'coefficient weight' to construct our inequivalent polynomials. It therefore follows that the number of inequivalent polynomials, d_n , satisfies,

$$d_n = 1 + m \sum_{k=1}^n \sum_{\text{hw}=1}^m \binom{k-1}{k-\text{hw}} e_{\text{hw},m} \quad (2)$$

For $m = 6$,

$$\begin{aligned}
d_0 &= 1 \\
d_1 &= 1 + 6 = 7 \\
d_2 &= 1 + 6 + 6(1 + 1) = 19 \\
d_3 &= 1 + 6 + 6(1 + 1) + 6(1 + 2 + 0) = 37 \\
d_4 &= 1 + 6 + 6(1 + 1) + 6(1 + 2 + 0) + 6(1 + 3 + 0 + 0) = 61 \\
d_5 &= 1 + 6 + 6(1 + 1) + 6(1 + 2 + 0) + 6(1 + 3 + 0 + 0) + 6(1 + 4 + 0 + 0 + 0) = 91 \\
&\dots \text{ etc}
\end{aligned}$$

These numbers agree with those of Table 1. The number of r -way ordered partitions adding to n is $p_r(n)$, and

$$p_r(n) = \binom{n+r-1}{n}$$

Therefore we can rewrite (2) in terms of partitions as,

$$d_n = 1 + m \sum_{k=1}^n \sum_{hw=1}^m p_{hw}(k-hw) e_{hw,m} \quad (3)$$

8.4 Comments on the Technique

The technique assumes that all polynomials in \mathbf{E} have cyclic order m . It seems likely that this is true in general as d_n appears to satisfy $m|(d_n - 1)$ for all cases computed in Tables 1 and 2. A proof of Conjecture 1, and a proof of the general form of $c_h(x)$ may well follow if one can do the following for a given m ,

1. Derive an efficient method to compute the 'forbidden' polynomials.
2. Derive an efficient method to compute the elements $e_{hw,m}$ of \mathbf{E} from the forbidden polynomials.

For large m (e.g. perhaps $m = 105$?) there may be non-binary forbidden polynomials for which the above technique must be modified as follows: Consider, as an example, a 'hypothetical' forbidden polynomial, $F(x)$, of the following form:

$$F(x) = x^5 + 3x^2 + x + 2$$

Then it has an associated binary forbidden polynomial, $f(x)$, where,

$$f(x) = x^5 + x^2 + x + 1$$

We wish to disallow all polynomials built from the foundation $F(x)$ not $f(x)$. Let the cyclic order (over m) of $F(x)$ and $f(x)$ be v . Then we should include γ_n polynomials in our count for d_n , where

$$\gamma_n = v \left(\sum_{k=1}^n p_4(k-4) - \sum_{k=1}^{n-3} p_4(k-4) \right) = v \sum_{k=n-2}^n p_4(k-4)$$

where the '3' in the summation limit of the previous equation is the coefficient weight (cw) of $F(x)$ minus the hamming weight of $F(x)$. In general, for a given forbidden polynomial $F(x)$ we include γ_n in our count for d_n where γ_n satisfies,

$$\gamma_n = v \sum_{k=n+\text{hw}(F(x))-\text{cw}(F(x))+1}^n p_{\text{hw}(F(x))}(k - \text{hw}(F(x)))$$

In the case where the forbidden polynomial is a binary polynomial $\text{hw}(F(x)) = \text{cw}(F(x))$ and γ_n for $F(x)$ is 0, as expected. Things will be further complicated if the cyclic order of $F(x)$ is lower than that of $f(x)$.

9 Acknowledgements

The author thanks S.J.Shepherd and D.A.Gillies for helpful discussions, and D.A.Gillies for writing software which independently confirmed results for the $m = 8$ case, and provided extra data for this case.

References

1. Parker, M.G.: VLSI Algorithms and Architectures for the Implementation of Number-Theoretic Transforms, Residue and Polynomial Residue Number Systems. **PhD thesis, School of Eng, University of Huddersfield, March 1995**
2. Safer, T.: Polygonal Radix Representations of Complex Numbers. *Theoretical Computer Science.* **210**, (1999) 159–171
3. Sloane, N.J.A.: An On-Line Version of the Encyclopedia of Integer Sequences. <http://www.research.att.com/njas/sequences/index.html>, *The Electronic Journal of Combinatorics.* **1**, (1994) 1–5
4. Conway, J.H., Sloane, N.J.A.: Low Dimensional Lattices VII: Coordination Sequences. *Proc. Royal Soc.* **A453** (1997) 2369–2389
5. O’Keeffe, M.: Coordination Sequences for Lattices. *Zeit. f. Krist.* **210**, (1995) 905–908
6. Grosse-Kunstleve, R.W., Brunner, G.O.: Algebraic Description of Coordination Sequences and Exact Topological Densities for Zeolites. *Acta Crystallographica. Section A.* **A52**, (1996) 879–889
7. Huber, K.: Codes Over Gaussian Integers. *IEEE Trans. on Inf. Theory.* **40**, No 1, Jan. (1994) 207–216
8. Huber, K.: Codes Over Eisenstein-Jacobi Integers. *Contemporary Mathematics.* **168**, (1994) 165–179