Self-dual spin 1/2 systems, zeros of partition function, error correcting codes

The last three pages of the present file have figures (‘end-figures’) with marked zeros of certain polynomials: partition functions of two (strongly) self-dual spin 1/2 systems with periodic boundary conditions and (Hamming) weight enumerators of ($[14, 7, 5]$ and $[30, 5, 6]$) cyclic self-dual binary (error correcting) codes.

Apart from the case of TT$[6, 6]$, all the zeros, with the exception of a few, are located on two circles (‘F-circles’): in the case of A6$[6, 10]$ only one zero (modulo the symmetry group of the figure) is off the F-circles.

In the following, we will discuss the systems in question, and we will argue that a unified treatment of both of them yields new insights into the problem of the location of the zeros and new (and interesting) codes.

Spin 1/2 Systems

The *energy* of a *(transitive, translation invariant)* spin $1/2$ ferromagnetic system on the lattice $\mathbb{Z}^d$ has the form

$$H \;=\; -\sum_{B\in\mathcal{B}} K(B)\sigma_B, \quad K(B) > 0\,,$$

where

$$\sigma_B \;=\; \prod_{a\in B}\sigma_a, \quad \sigma_a = \pm 1\,,$$

$\mathcal{B}$ is a translation invariant family of finite subsets, with a finite fundamental subfamily $\mathcal{B}_0$ generating it by translations. The *coupling constants* (*interaction*) $K(B)$ are proportional to inverse temperature.

Univariate version: all the coupling constants are equal.

Examples: The figures show a *fundamental family* $\mathcal{B}_0$ *of bonds*.

– Ising Model (IM)

– TT Model (solved by Baxter and Wu)

– A6 Model

• **Partition function.** For a finite subsystem Λ of the infinite system,

$$Z \;=\; Z_\Lambda(K) = \sum_{\boldsymbol{\sigma}} \exp(-H_{_\Lambda}(\boldsymbol{\sigma}))$$

$$\;=\; \sum_{\sigma_a=\pm 1, a\in\Lambda} \exp \sum_{B\in\mathcal{B}_\Lambda} K(B)\sigma_B\,,$$

$\mathcal{B}_\Lambda := \{B \in \mathcal{B} : B \subset \Lambda\}$. Here finite volumes Λ will be taken with *periodic boundary conditions* (‘periodic version of the model’). For example, we may take $\Lambda = \mathbb{Z}_m \times \mathbb{Z}_n$ in two dimensions. We will denote this periodic version by suffix $[m, n]$: TT$[6, 9]$ is the TT model on $\Lambda = \mathbb{Z}_6 \times \mathbb{Z}_9$, with periodic boundary conditions.

■ **The main result for IM** (1941). Define the *dual* interaction $\mathbf{K}^* = (K_1^*, K_2^*)$ by

$$\tanh K_1^* \;=\; \exp -2K_2, \quad \tanh K_2^* = \exp -2K_1$$

Then

$$P(\mathbf{K}) - \frac{1}{2}\ln\prod_i \cosh 2K_i \;=\; P(\mathbf{K}^*) - \frac{1}{2}\ln\prod_i \cosh 2K_i^*$$

($P = \lim_\Lambda |\Lambda|^{-1} \ln Z_\Lambda$)

Corollary (location of the critical point). *For equal coupling constants*, $K_1 = K_2 = K$

$$\tanh K = \exp -2K \quad \Rightarrow \quad K_{\mathrm{cr}} = \frac{1}{2}\ln\left(\sqrt{2}+1\right)$$

(This is the IM first exact result, showing, in particular, that a number of results obtained through approximate calculations cannot be true)

General Formulation of Duality (1971+).

For any finite set Λ and a family $\mathcal{B}$ of its subsets, introduce

$$\text{configuration space} \quad \Omega = \Omega_\Lambda := \{-1, 1\}^\Lambda;$$

$\gamma : \Omega \to \mathcal{P}(\mathcal{B})$ (contour map),

$$\gamma(\sigma) := \{B \in \mathcal{B} : \sigma_B = -1\}, \quad \Gamma := \mathrm{Im}\,(\gamma)$$

$$\mathcal{K} := \{\beta \subset \mathcal{B} : \prod_{B \in \beta} \sigma_B = 1, \ \forall \boldsymbol{\sigma} \in \Omega\}$$

$$\mathcal{S} := \{\sigma : \sigma_B = 1, \forall B \in \mathcal{B}\} = \{\sigma : \gamma(\sigma) = \emptyset\}$$

elements of Γ, $\mathcal{K}$, Ω and $\mathcal{S}$ are called *contours*, *cycles*, *configurations* and *ground states*, respectively. $|\mathcal{S}| = 2$ for IM, $|\mathcal{S}| = 4$ for the TT model, and $|\mathcal{S}| = 16$ for the A6 model. These definitions are extended to infinite Λ in appropriate way.

• **Low and High Temperature Expansions** Introduce the polynomials

$$Z^{\mathrm{LT}} = Z_\Lambda^{\mathrm{LT}}(w) = \sum_{\beta\in\Gamma} w^\beta, \quad w^\beta = \prod_{B\in\beta} w_B,$$

and

$$Z^{\mathrm{HT}} = Z_\Lambda^{\mathrm{HT}}(x) = \sum_{\beta\in\mathcal{K}} x^\beta, \quad x^\beta = \prod_{B\in\beta} x_B\,.$$

When $w_B = e^{-2K(B)}$ and $x_B = \tanh K(B)$ both are equal to the partition function, up to trivial factors, yielding, respectively, its Low and High Temperature Expansions.

(Finite) system is *self-dual* when the two polynomials are equal, *strongly self-dual* if $\mathcal{K} = \Gamma$

With the natural group structures on Ω and $\mathcal{P}(\mathcal{B}) \simeq \mathbb{F}_2^{\mathcal{B}}$ ($\mathbb{F}_2 = \{0, 1\}$ is the two-element field), σ_B become characters; γ a homomorphism; $\mathcal{S} \subset \Omega$, $\Gamma \subset \mathcal{P}(\mathcal{B})$ and $\mathcal{K} \subset \mathcal{P}(\mathcal{B})$ subgroups.

Moreover, for $\Lambda = \mathbb{Z}^d$, translations act in a natural way by homomorphisms on each of these groups. For infinite systems one has:

Definition. A system is *self-dual* if there is a bijection $\mathcal{B} \to \mathcal{B}$ which *commutes* or *anticommutes* with translations and defines an isomorphism of Γ onto $\mathcal{K}$. A system is *strongly self-dual* if $\mathcal{K} = \Gamma$.

Theorem. A spin 1/2 system on a lattice $\mathbb{Z}^d$, any dimension d, is self-dual if and only if $|\mathcal{B}_0| = 2$. It is strongly self-dual if and only, with $\mathcal{B}_0 = \{B_1, B_2\}$, B_2 is a translation of $I(B_1)$, where

$$I(B) = \{-a : a \in B\}\,.$$

Thus, while all three models of p. 4 are self-dual, only the last two are strongly self-dual.

F(isher's)-zeros

These are the zeros of $Z^{\mathrm{LT}}(w)$ – the main object of the present study. They are, in a sense, of a more combinatorial nature than Lee-Yang zeros.

• Fisher (1964): for IM (no external field, in infinite volume limit), *F-zeros are on the circles*

$$|w-1| = \sqrt{2}, \quad |w+1| = \sqrt{2}$$

(F-circles). It was shown later that this holds for finite IM with suitable boundary conditions.

For finite IM with periodic boundary conditions, most of the F-zeros are off the F-circles, as in the case of TT [6,6].

• For the models considered below, the set of zeros is symmetric under the group (D_{16}) generated by

$$Dx = \frac{1-x}{1+x}, \quad Ix = \frac{1}{x}, \quad Cx = x^*$$

Invariance under D follows from self-duality; invariance under I follows from *palindromicity* of Z.

Strongly Self-dual Systems with periodic boundary conditions

One has $\mathcal{B} = \mathcal{B}_\Lambda, \Gamma, \mathcal{K} \subset \mathcal{P}(\mathcal{B}) \simeq \mathbb{F}_2{}^{\mathcal{B}}$,

$$\mathcal{K} = \Gamma^\perp, \quad \Gamma = \mathcal{K}^\perp$$

where orthogonality is with respect to the bilinear form on $\mathbb{F}_2{}^{\mathcal{B}}$:

$$(\alpha, \beta) \mapsto \alpha \cdot \beta := \sum_{B \in \mathcal{B}} \alpha_B \beta_B$$

(sum in $\mathbb{F}_2$). By linear algebra,

$$\dim_{\mathbb{F}_2} \Gamma + \dim_{\mathbb{F}_2} \mathcal{K} = |\mathcal{B}| \ .$$

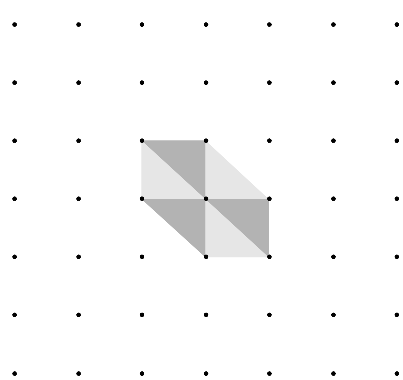
Since $2^{|\Lambda|} = |\mathcal{S}| \cdot |\Gamma|$ ($\mathcal{S} = \mathrm{Ker}\, \gamma$, $\Gamma = \mathrm{Im}\, \gamma$!), this implies that a periodic version of a strongly self-dual model is (strongly) self-dual if and only if $\mathcal{S}$ is trivial. Equivalently, if and only if no ground state, apart from the trivial one, has the periodicity of Λ. Hence one has to consider only *systems with* $|B|$ *odd*.[1]

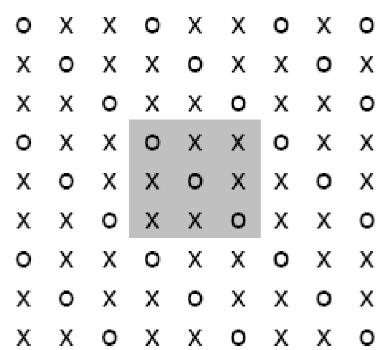
[1] If $\mathcal{S}$ is non-trivial, a quantum code that can be defined by these systems can correct $|\mathcal{S}|^2$ errors.

In 2D, (after possibly reducing the system, in a suitable sense) the *number of ground states is finite*, and for any strongly self-dual system with $|B|$ odd, there exist a sequence of $\Lambda_n \to \mathbb{Z}^2$ for which the Λ_n-versions of the system are (strongly) self-dual.

Example. TT$[5, 6]$ model is (strictly) self-dual, while TT$[6, 6]$ or TT$[6, 9]$ are not. More generally, TT$[m, n]$ model is self-dual unless both m and n are multiples of three. The end-figures show that in the TT$[5, 6]$-case, the zeros are on the F-circles while in the TT$[6, 6]$-case they are not.

The first of the figures





shows a generator of both Γ and $\mathcal{K}$, while the second one shows a ground state of the model on $\mathbb{Z}^2$: o stands for $+1$ and $\times$ for -1. Translating it, one obtains the other two non-trivial ground states. That no TT$[m, n]$ system has non-trivial ground states, unless both m and n are multiples of three, follows from periodicity properties of this ground state.

From theory of Linear Binary Codes:

Binary code C of length n = subspace of $\mathbb{F}_2^n$. For $c \in C$, the *weight* of c is

$$\mathrm{wt}\,(c) = \text{number of nonzero components of } c.$$

(Hamming) weight enumerator $W_C(X,Y)$ of the code C is the homogeneous polynomial

$$\begin{aligned} \mathrm{hwe}_C(X,Y) \; &= \; W_C(X,Y) = \sum_{c \in C} X^{n-\mathrm{wt}(c)} Y^{\mathrm{wt}(c)} \\ &= \sum_{m=0}^{n} N_m(C) X^{n-m} Y^m \,, \end{aligned}$$

where $N_m(C)$ is the number of codewords of weight m, which is the homogeneous form of the polynomial

$$W_C(z) = \sum_{c \in C} z^{\mathrm{wt}(c)},$$

zeros of which are shown on the end-figures.

Dual code

$$C^{\perp} = \{c \in \mathbb{F}_2^n : c \cdot c' \equiv 0, \forall c' \in C\} \,.$$

A code is *self-dual* if it is equal to its dual.

Lattice associated with self-dual codes

The *lattice* $L_C \subset \mathbb{R}^n$ is defined by integer vectors that reduce mod 2 to codewords,

$$L_C := \{2^{-1/2}v : v \in \mathbb{Z}^n, v \mod 2 \in C\}.$$

The lattice *dual* to L_C is the lattice $L_{C^\perp}$ of the dual code. Hence the lattice of self-dual codes are *unimodular*.

- Theta series of a code C is the theta series of L_C:

$$\Theta_C(z) = \Theta_{L_C}(z) := \sum_{k \in L_C} z^{k \cdot k} .$$

Theta series of a code is related to its weight enumerator:

$$\Theta_C = W_C(\Theta_0, \Theta_1) ,$$

where

$$\Theta_0(z) := \sum_{k \in \mathbb{Z}} z^{2k^2}, \quad \Theta_1(z) := \sum_{k \in \mathbb{Z}} z^{2(k+1/2)^2}.$$

For a self-dual code $\theta_C(\tau) := \Theta_C(e^{i\pi\tau})$ is a modular form for the group $\Gamma(2)$.

Full weight enumerators can be expressed through Siegel modular form.

• *Cyclic codes*. C is invariant under cyclic permutations of its elements:

$$\begin{aligned}(c_0, c_1, \ldots, c_{n-2}, c_{n-1}) \;\in\; C \quad \Rightarrow \\ (c_{n-1}, c_0, c_1, \ldots, c_{n-2}) \;\in\; C\end{aligned}$$

Equivalent formulation: For $c \in C$, let

$$c(T) := \sum_{i=0}^{n-1} c_i T^i \in R = \mathbb{F}_2[T]/\left\langle T^n - 1\right\rangle$$

then $\{c(T) : c \in C\}$ is a (principal) ideal of R. Let $g(T)$ be a generator of the ideal; the code is self-dual if and only if

$$I(g)(T) \cdot g(T) \equiv 0 \mod(T^n - 1)\,.$$

For example, the first two end-figures show zeros of $W_{[14,7,4]}(z)$ and $W_{[30,15,6]}(z)$, which are the weight enumerator of the cyclic self-dual codes denoted $[14, 7, 4]$ (length 14) and $[30, 15, 6]$ (length 30), respectively. The ideal of the $[14, 7, 4]$ code is generated by

$$g(T) \;=\; 1 + T + T^2 + T^3 + T^6 + T^7;$$

$I(g)(T)$, usually denoted $\overleftarrow{g}\,(T)$, is $1+T+T^4+T^5+T^6+T^7$, with $\overleftarrow{g}\,(T) \cdot g(T) \equiv 0 \mod(T^{14} - 1)$.

More examples of cyclic self-dual codes (‘trivial’): $n = 2m$, $g(T) = 1 + T^n$. AN easy calculation yields

$$\begin{aligned} W(X, Y) \;&=\; (X^2 + Y^2)^m = X^{2m}(1 + z^2)^m \\ &=\; X^{2m}(z - i)^m(z + i)^m = X^{2m}W(z). \end{aligned}$$

This yields $z = \pm i$ for roots of $W(z)$, roots that appear on all the end-figures.

Strongly self-dual spin systems yield (new) self-dual multi-cyclic codes

Setting $C = \Gamma$ one obtains a binary (multi-)cyclic code of length $|\mathcal{B}|$ ('contour codes'). The map $\gamma : \{-1, +1\}^{\Lambda} \to \mathbb{F}_2^{\mathcal{B}}$ yields a coding. The code is self-dual if and only if the spin system is strongly self-dual. Translation invariance of the spin system implies multi-cyclicity of the code.

As $|\Lambda|$ is increased, one obtains a family of self-dual regular low-density parity-check codes (LDPC), codes that are known to exhibit good performance under message-passing decoding.

The partition function of the spin system is equal to the weight enumerator of the code:

$$Z^{\mathrm{LT}}(w) \ = \ W_{\Gamma}(w) = \frac{\Theta_{L_\Gamma}(w)}{\Theta_0(w)^{|\mathcal{B}|}} = \frac{\theta_{L_\Gamma}(\tau)}{\theta_0(\tau)^{|\mathcal{B}|}}\,,$$

$w = \theta_1(\tau)/\theta_0(\tau)$, and the celebrated MacWilliams Theorem about relation between $W_{C^\perp}$ and W_C is an expression of LT-HT duality discussed earlier.[2]

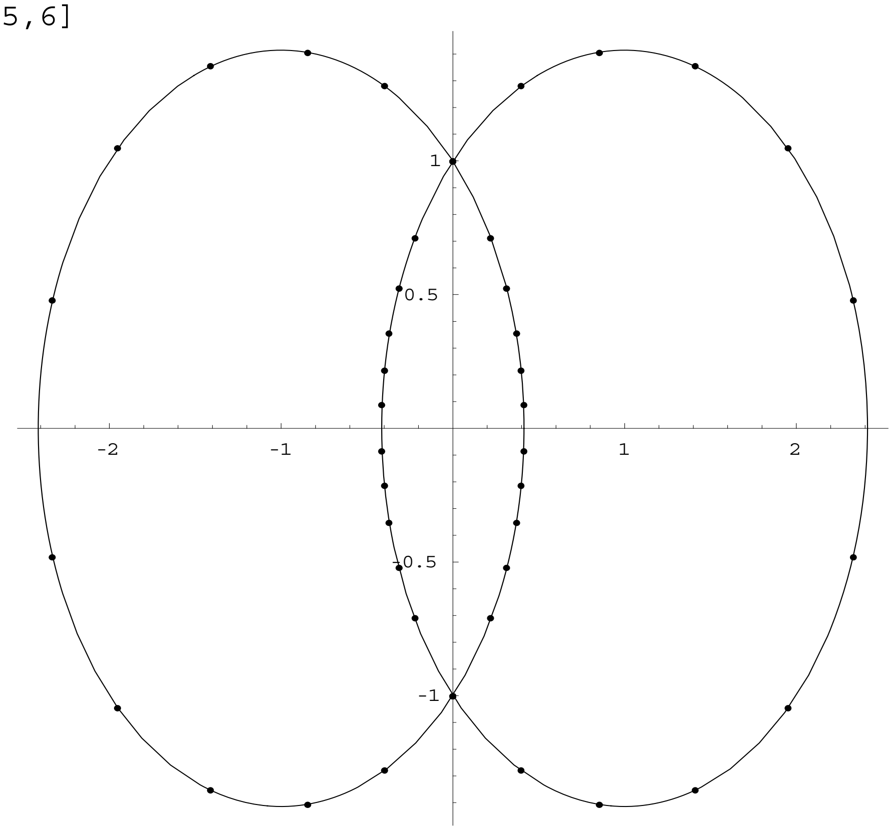
[2] The cyclic codes are a degenerate case of contour codes: they are obtained when $\mathcal{B}_0$ has just one element, say B, instead of two, and the pair (B, Λ) satisfies the condition $I(B) \cdot B \equiv 0 \in \mathbb{F}_2\Lambda$.

Thus, on the one hand one obtains an expression of the partition function of spin systems in terms of an exponential of a quadratic form and a modular function; on the other hand, one obtains a new family of self-dual LDPC. [3]

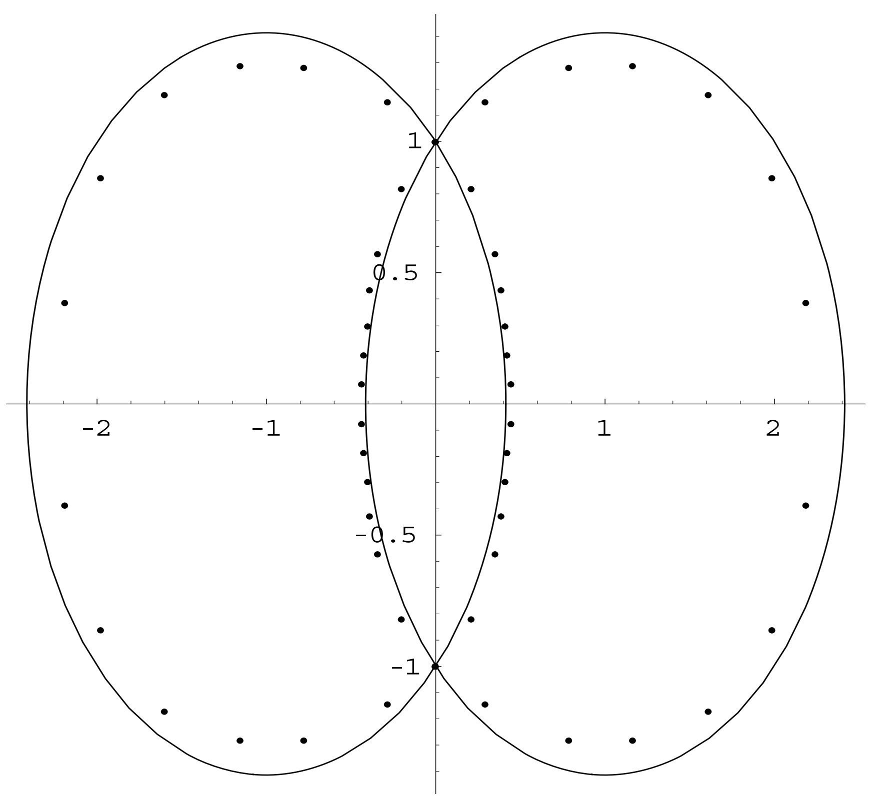
This structure (and its generalization to the non-binary case, and lattices more general than $\mathbb{Z}^d$), relating spin systems and (multi-)cyclic codes, is currently being exploited in analysis of zeros of partition function and properties of the corresponding codes.

[3] The counter-image of the F-circles under the map $\tau \mapsto w$ of $\mathbb{H}$ to $\mathbb{C}$ consists of a nice family of semi-circles (geodesics).

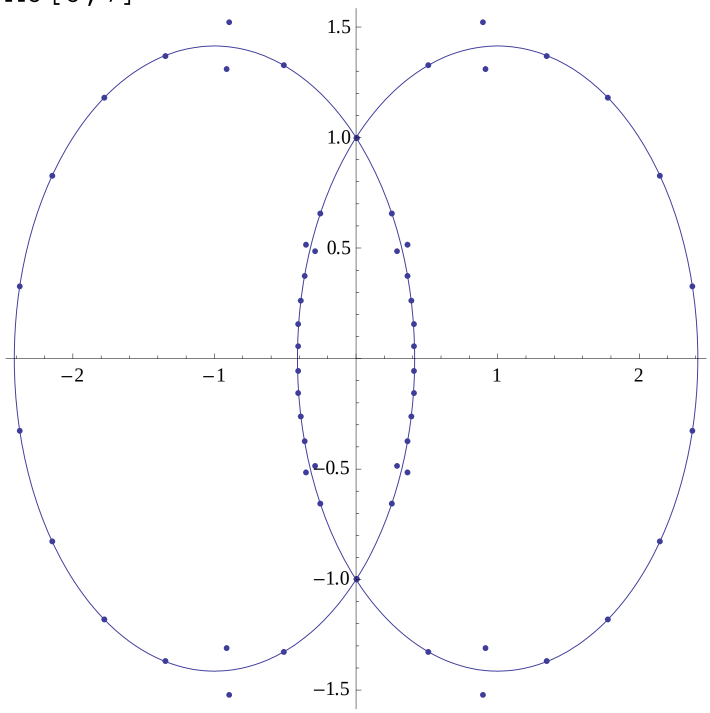
ATT[5,6]



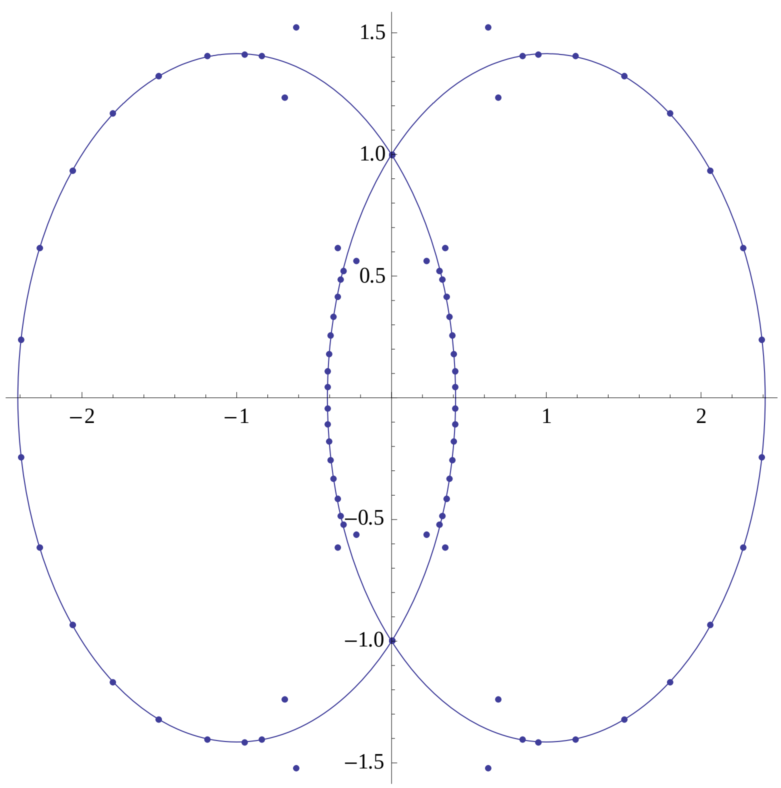
ATT[6,6]



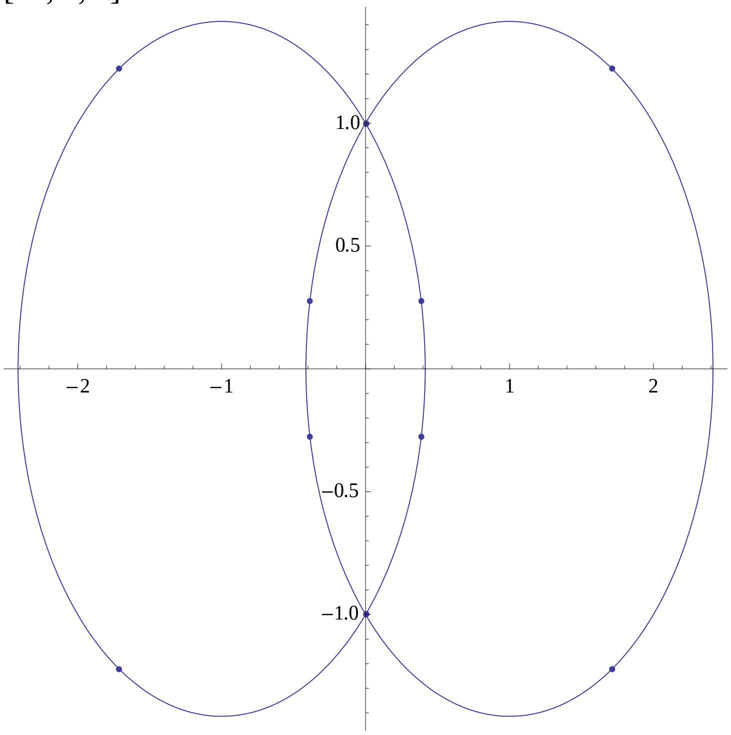
A6[6,7]



A6[6,10]



[14, 7, 4]



[30,15,6]