On the problem of PCE's

We have the matrix

$$M = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix} \tag{1}$$

which satisfies the obvious relation

$$M^{-1} = \frac{1}{2} M \tag{2}$$

We wish to find those vectors consisting of 0's and 1's such that

$$M^{\otimes N} \vec{\sigma} \tag{3}$$

is a vector with positive entries. Here $\vec{\sigma}$ is a 4^N dimensional vector of 0's and 1's. We number the entries of $\vec{\sigma}$ by the multi-indices $\vec{\alpha} = (\alpha_1, \ldots, \alpha_N)$ where $0 \leq \alpha_k \leq 4$. The entries of the positive vector are given by $2^N p_{\vec{\alpha}}$. It then follows that the expression (3) satisfies

$$\left(M^{\otimes N}_{\vec{\alpha}\vec{\beta}} \right) \sigma_\beta = 2^N p_\alpha \tag{4}$$

where clearly

$$\left(M^{\otimes N}_{\vec{\alpha}\vec{\beta}} \right) = M_{\alpha_1 \beta_1} \cdot \ldots \cdot M_{\alpha_N \beta_N} \tag{5}$$

From (4) immediately follows, via (2)

$$\sigma_\alpha = \left(M^{\otimes N}_{\vec{\alpha}\vec{\beta}} \right) p_\beta \tag{6}$$

which we analyze iteratively. We shall essentially use the fact that

$$p_{\vec{\alpha}} + p_{\vec{\beta}} = 0 \quad \Leftrightarrow \quad p_{\vec{\alpha}} = p_{\vec{\beta}} = 0 \tag{7}$$

Now we need a definition: to each multi-index $\vec{\alpha}$ we associate a *set* of multi-indices $\Phi(\vec{\alpha})$ as follows

$$\Phi(\vec{\alpha}) := \left\{ \vec{\beta} : \left(M^{\otimes N} \right)_{\vec{\alpha}\vec{\beta}} = 1 \right\} = \left\{ \vec{\beta} : M_{\alpha_1 \beta_1} \cdot \ldots \cdot M_{\alpha_N \beta_N} = 1 \right\} \tag{8}$$

If we now assume that $\sigma_{\vec{\alpha}} = 1$, it follows from subtracting the two combined equations

$$\sum_{\vec{\beta}} p_{\vec{\beta}} \quad = \quad 1 \tag{9a}$$

$$\sum_{\vec{\beta}} \left(M^{\otimes N} \right)_{\vec{\alpha}\vec{\beta}} p_{\vec{\beta}} \quad = \quad \sigma_{\vec{\alpha}} = 1 \tag{9b}$$

that for all $\vec{\beta} \notin \Phi(\vec{\alpha})$

$$p_{\vec{\beta}} = 0. \tag{10}$$

From this follows that $\sigma_{\vec{\alpha}} = 1$ implies various equalities between the remaining $\sigma_{\vec{\gamma}}$. Indeed, let

$$\left(M^{\otimes N}\right)_{\vec{\beta}\vec{\gamma}} = \left(M^{\otimes N}\right)_{\vec{\beta}\vec{\gamma}'} \tag{11}$$

hold for all $\vec{\beta} \in \Phi(\vec{\alpha})$. If this condition is fulfilled and $\sigma_{\vec{\alpha}} = 1$, then

$$\begin{aligned}
\sigma_{\vec{\gamma}} &= \sum_{\vec{\beta}} \left(M^{\otimes N}\right)_{\vec{\beta}\vec{\gamma}} p_{\vec{\beta}} && \text{(12a)}\\
&= \sum_{\vec{\beta}\in\Phi(\vec{\alpha})} \left(M^{\otimes N}\right)_{\vec{\beta}\vec{\gamma}} p_{\vec{\beta}} && \text{(12b)}\\
&= \sum_{\vec{\beta}\in\Phi(\vec{\alpha})} \left(M^{\otimes N}\right)_{\vec{\beta}\vec{\gamma}'} p_{\vec{\beta}} && \text{(12c)}\\
&= \sum_{\vec{\beta}} \left(M^{\otimes N}\right)_{\vec{\beta}\vec{\gamma}'} p_{\vec{\beta}} && \text{(12d)}\\
&= \sigma_{\vec{\gamma}'} && \text{(12e)}
\end{aligned}$$

Here the transition from (12a) to (12b) follows from (10), from (12b) to (12c) follows from (11), from (12c) to (12d) follows again from (10).

Condition (11) combined with $\sigma_{\vec{\alpha}} = 1$ therefore implies $\sigma_{\vec{\gamma}} = \sigma_{\vec{\gamma}'}$. Since $M_{\alpha\beta} = \pm 1$, we may rewrite (11) as

$$M_{\beta_1\gamma_1} M_{\beta_1\gamma_1'} \cdot \ldots \cdot M_{\beta_N\gamma_N} M_{\beta_N\gamma_N'} = 1. \tag{13}$$

This must hold for all $\vec{\beta} \in \Phi(\vec{\alpha})$. From this follows that (13) may be rewritten as

$$M_{\beta_1\gamma_1} M_{\beta_1\gamma_1'} \cdot \ldots \cdot M_{\beta_N\gamma_N} M_{\beta_N\gamma_N'} = M_{\alpha_1\beta_1} \cdot \ldots \cdot M_{\alpha_N\beta_N}. \tag{14}$$

Since this must hold for all $\vec{\beta} \in \Phi(\vec{\alpha})$, it follows that for all $1 \leq k \leq N$, γ_k and γ_k' are so related that

$$M_{\beta\gamma_k} M_{\beta\gamma_k'} = M_{\beta\alpha} \tag{15}$$

for all $0 \leq \beta \leq 3$. This is equivalently expressed as

$$M_{\beta\gamma_k'} = M_{\beta\gamma_k} M_{\beta\alpha} \tag{16}$$

which we further express as

$$\gamma_k' = \alpha \oplus \gamma_k \tag{17}$$

where the $\oplus$ operation is defined by (16). See Figure 1 for a detailed description.

Now everything follows with delightful simplicity. First extend the $\oplus$ operation to vectors componentwise

$$\vec{\alpha} \oplus \vec{\beta} = (\alpha_1 \oplus \beta_1, \ldots, \alpha_N \oplus \beta_N). \tag{18}$$

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Figure 1: Table for the $\oplus$ operation defined in (16). Note that the operation is an *abelian group*, in fact it corresponds to the *Klein group*, where the neutral element is 0. This is the reason for choosing an additive notation for the operation defined in (16).

Remark, as a useful fact, that the inverse under $\oplus$ of any number α is α itself.

If $\sigma_{\vec{\alpha}} = 1$, then it follows from the above that for all γ

$$\sigma_{\vec{\gamma}} = \sigma_{\vec{\alpha}\oplus\vec{\gamma}}. \tag{19}$$

So we may now proceed to generate all solutions: we start out from the solution having $\sigma_{\vec{0}} = 1$, with everything else 0. We may then successively switch σ's to 1 for various values of $\vec{\alpha}$, taking care immediately to set equal to one the values of σ that correspond to values of $\vec{\beta}$ generated by the previously switched values of $\vec{\alpha}$ via (19).

We may now interpret this a bit differently: (19) states that the set of all $\vec{\alpha}$'s for which $\sigma_{\vec{\alpha}} = 1$ is closed under the operation $\oplus$. But the set V of all vectors $\vec{\alpha}$ with $0 \leq \alpha_k \leq 3$ form a vector space over the field with 2 elements $\{0, 1\}$. Here the addition of 2 vectors is given by $\oplus$ and the multiplication by a scalar is given by

$$0 \cdot \vec{\alpha} = 0, \qquad 1 \cdot \vec{\alpha} = \vec{\alpha}. \tag{20}$$

The dimension of the vector space is $2N$, and the condition (19) states that

$$W = \{\vec{\alpha} : \vec{\alpha} \in V, \sigma_{\vec{\alpha}} = 1\} \tag{21}$$

is a subspace of V. As such, W has a given dimension K, which means that W has 2^K elements, or in other words, that the 2^K rule holds.

By standard theorems of linear algebra, any subspace W can be extended to a maximal (non-trivial) subspace of dimension $2N - 1$ by adjoining appropriate additional basis elements. This can clearly be done in different ways. We therefore arrive to the set of maximal extensions of W. Clearly, the intersection of all the elements of this set reduces to W itself, leading to the claimed result that all PCE's can be obtained as intersections of maximal PCE's.

Finally, we may enumerate straightforwardly the subspaces W of dimension K. We do this in 2 steps: first, we evaluate $\mathcal{N}_{K,N}$, the number of all bases of K elements. Each of these corresponds to one subspace of dimension K, but each subspace corresponds to a number $\mathcal{M}_K$ of different bases. The crucial point is that $\mathcal{M}_K$ is independent of the subspace under consideration: $\mathcal{M}_K$ simply describes the number of linear maps of W onto itself. The total number $\mathcal{S}_{N,K}$ of subspaces of dimension K is therefore $\mathcal{N}_{N,K}/\mathcal{M}_K$.

To evaluate $\mathcal{N}_{N,K}$ we proceed by steps: the first element of the basis can be any non-zero element, of which the number is $2^{2N}-1$. The second element must be chosen not belonging to the subspace generated by the first basis element. Of these there are $2^{2N}-2$. Generally, for the basis element $m+1$, we must choose from those which do not belong to the m dimensional space generated by the first m basis elements, so that one chooses from $2^{2N}-2^m$. We thus have

$$\mathcal{N}_{N,K} = \prod_{m=0}^{K-1} \left(2^{2N}-2^m\right). \tag{22}$$

On the other hand, the maps of a K-dimensional vector space W onto itself is described by a non-singular binary $K\times K$ matrix over the field $\{0,1\}$. To count these, we proceed as above: the first line is an arbitrary non-zero vector, of which there are 2^K-1. For the row $m+1$ we must choose an arbitrary vector not belonging to those generated by the first m vectors, of which there are 2^K-2^m. This eventually yields

$$\mathcal{M}_K = \prod_{m=0}^{K-1} \left(2^K-2^m\right). \tag{23}$$

From this follows that

$$\mathcal{S}_{N,K} = \prod_{m=0}^{K-1} \frac{2^{2N-m}-1}{2^{K-m}-1}. \tag{24}$$

An elementary test is $N=3$ and $K=2,3$:

$$\begin{aligned}
\mathcal{S}_{3,2} &= \frac{(2^6-1)(2^5-1)}{(2^2-1)(2^1-1)} = \frac{63\cdot 31}{3} = 651, &(25)\\
\mathcal{S}_{3,3} &= \frac{(2^6-1)(2^5-1)(2^4-1)}{(2^3-1)(2^2-1)(2^1-1)} = \frac{63\cdot 31\cdot 15}{7\cdot 3} = 1395, &(26)
\end{aligned}$$

which are indeed the values found numerically.

The symmetry suggested in the paper

$$\mathcal{S}_{N,K} = \mathcal{S}_{N,2N-K} \tag{27}$$

can also be proved with a bit of algebra from (24).