I. PROOF

Goal: Choose n binary numbers such that the MAC number denoted as

$$MAC_{a,b} = \frac{(\mathbf{a} \cdot \mathbf{b})^2}{(\mathbf{a} \cdot \mathbf{a})(\mathbf{b} \cdot \mathbf{b})} \tag{1}$$

is minimized for every combination of numbers a and b including their the corresponding cyclically shifted versions.

Consider an n bit binary number greater than zero with p ones and $n-p$ zeros, where $0 < p < n$. Further, shift this number by any number of bits so that the left-most bit contains a one. Because of the cyclic nature, the binary number can be written as a vector containing the integer number of zeros bounded on either end by ones. For example, the number 0 1 1 would be shifted to 1 0 1 and could be written as the vector [1]. Also, the number [0 1 0 1 0 1 0 0] can be shifted to [1 0 1 0 1 0 0 0], and the corresponding vector is [1 1 3]. Recall that the vector's cyclic nature causes the last one to wrap around to the first position. In general, we can write any non-zero binary number as the vector $\mathbf{v} = [v_1\ v_2\ v_3\ \cdots\ v_p]$, where each v_i is the number of zeros between two ones and $v_p = n - p - \sum_i v_i$.

Now, cyclic redundancy can be avoided by ignoring any $\mathbf{v}$ that become duplicated under shifts. For example, [0 3 2] and [3 2 0] represented the same binary number, where the second vector is the first shifted to the left by $v_1 + 2$ bits. To avoid this behavior, we require $v_1 < v_p$, but $v_2 \leq v_p, v_3 \leq v_p, \cdots, v_{p-1} \leq v_p$. Note that by construction two vectors with a different number of ones cannot be cyclically identical.

Consider two vectors, $\mathbf{u} = [u_1\ u_2\ u_3\ \cdots\ u_{p_u}]$ and $\mathbf{v} = [v_1\ v_2\ v_3\ \cdots\ v_{p_v}]$ containing p_u and p_v ones respectively. If $u_i = v_i$ the vector has at least two ones in the corresponding binary number that would align for some shift of $\mathbf{u}$. We want to choose n vectors, which $a_1, a_2, ...a_n$ that produce the minimum value of $max\{MAC_{a_1...a_n}\}$, where the maximum is taken over all possible shifts of $\mathbf{a}_i, \mathbf{a}_j$, $i = 1...n$, and $j = 1...n$. Note that if $i = j$, then the second vector must be shifted by at least one bit to avoid comparing a vector with itself. For a binary number undergoing all possible shifts, the denominator becomes $p_u * p_v$, while the numerator is the square of the total number of ones that simultaneously align as each vector is rotated. As the number of ones increases, both the numerator and denominator increase. Thus, it becomes unclear if the MAC number increases or decreases as p_u and/or p_v increase.

First, consider $p = 1$. There is only one vector, which can be expressed as $[n-1]$. There are no other possible non-cyclically redundant combinations. Letting a and b be this vector results in a maximum MAC number of $\frac{0}{1*1} = 0$.

Next, consider $p = 2$. Possible vectors include $[0\ n-p], [1\ n-p-1], [2\ n-p-2], \cdots, [\frac{n-p-1}{2}\ \ \frac{n-p+1}{2}]$ if n is odd or a limit of $[\frac{n-p}{2} - 1\ \ \frac{n-p}{2} + 1]$ if n is even. Note that there are only $\frac{n-p+1}{2}$ if n is odd and $\frac{n-p}{2}$ if n is even possible vectors of type $p = 2$, but n are required. Thus, more vectors from other p types would be required to complete the basis set. By construction, all of the indices are unique indicating that only one 1 aligns over all possible rotations (if two aligned, then the vectors would in fact be identical). Thus, the maximum MAC number, when using any two $p = 2$ vectors is $\frac{1^2}{2*2} = 1/4$.

Consider $p = 3$. Let $m = \lfloor \frac{n-p-1}{p} \rfloor$, $q = \lfloor \frac{n-p}{2} \rfloor$, and s is 0 if n is odd and 1 if n is even. The possible vectors are sets of decreasing size

$$\{[0,\ 0,\ n-p-0]; [0,\ 1,\ n-p-1]; \cdots [0,\ q-0,\ q+s-0]\},$$

$$\{[1,\ 0,\ n-p-1];[1,\ 1,\ n-p-2];\cdots[1,\ q+s-1,\ q-0]\},$$
$$\{[2,\ 0,\ n-p-2];[2,\ 1,\ n-p-3];\cdots[2,\ q-1,\ q+s-1]\},$$
$$\{[3,\ 0,\ n-p-3];[3,\ 1,\ n-p-4];\cdots[3,\ q+s-2,\ q-1]\},$$
$$\{[4,\ 0,\ n-p-4];[4,\ 1,\ n-p-5];\cdots[4,\ q-2,\ q+s-2]\},$$
$$\vdots$$
$$\{[m,\ 0,\ n-p-m],[m,\ 1,\ n-p-m-1],\cdots[m,\ q-\lfloor\tfrac{m+1}{2}\rfloor+s\ mod(m,2),\ q-\lfloor\tfrac{m}{2}\rfloor+s\ mod(m+1,2)]\},$$

In general, the kth set can be expressed as

$$\{[k,\ 0,\ n-p-k],[k,\ 1,\ n-p-k-1],\cdots[k,\ q-\lfloor\frac{k+1}{2}\rfloor+s\ mod(k,2),\ q-\lfloor\frac{k}{2}\rfloor+s\ mod(k+1,2)]\}, \tag{2}$$

where the total number of terms, t_1, is

$$t_1=\sum_{k=0}^{m}\lfloor\frac{n-p}{2}\rfloor-\lfloor\frac{k+1}{2}\rfloor+s\ mod(k,2)+1. \tag{3}$$

Since $v_1<v_3$, sets with $v_1>m$, can be expressed using the following approach,

$$\{[m+1,\ 0,\ n-p-m-1];[m+1,\ 1,\ n-p-m-2];\cdots[m+1,\ n-p-2m-3,\ m+2]\},$$
$$\{[m+2,\ 0,\ n-p-m-2];[m+2,\ 1,\ n-p-m-3];\cdots[m+2,\ n-p-2m-5,\ m+3]\},$$
$$\{[m+3,\ 0,\ n-p-m-3];[m+3,\ 1,\ n-p-m-4];\cdots[m+3,\ n-p-2m-7,\ m+4]\},$$
$$\vdots$$
$$\{[\lfloor\tfrac{n-p-1}{2}\rfloor,\ 0,\ q+1]\}\text{ if }n\text{ is even.}$$
$$\{[\lfloor\tfrac{n-p-1}{2}\rfloor,\ 0,\ q+1];[\lfloor\tfrac{n-p-1}{2}\rfloor,\ 1,\ q]\text{ if }n\text{ is odd.}$$

In general, the kth set can be expressed as

$$\{[k,\ 0,\ n-p-k-0],[k,\ 1,\ n-p-k-1],\cdots[k,\ n-p-2k-1,\ k+1]\}, \tag{4}$$

where the total number of terms, t_2, is

$$t_2=\sum_{k=m+1}^{\lfloor\frac{n-p-1}{2}\rfloor}n-p-2k-1+1=\sum_{k=m+1}^{\lfloor\frac{n-p-1}{2}\rfloor}n-p-2k \tag{5}$$

Thus, the total number of terms for n and $p=3$ is $t=t_1+t_2$. Note that the $p=1$ vector can be combined with the $p=3$ vectors, since the maximum MAC number between a $p=1$ and $p=3$ vector is $\frac{1^2}{1*3}=1/3<4/9$ (only one "1" can align). Figure 1 shows that the number of possible terms (including $p=1$) equals ($n=8$) or exceeds n ($8<n\leq 360$). Due to manufacturing constraints, n was limited to 360 as this corresponds to one degree increments in θ and 0.5 degree in ϕ. As a result, a full basis can be formed from these vectors if $n>7$.

Now, consider creating a $p>3$ basis. Let r represent the greatest number of repeated indices for any two basis vectors.

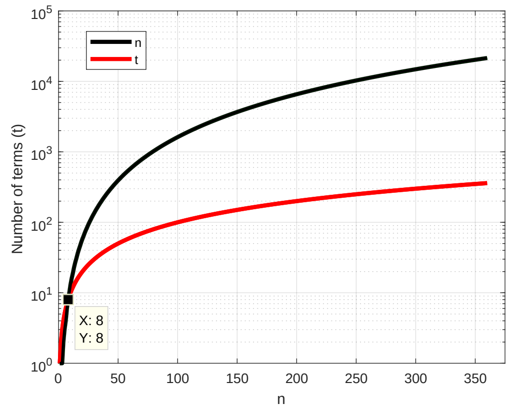

Fig. 1. The number of possible terms for $p = 1$ and 3 equals or exceeds n if $n > 7$.

The maximum MAC number can then be expressed as

$$MAC_{a,b} = \frac{r^2}{p_a p_b}, \tag{6}$$

where p_a and p_b are the p-type of vectors a and p respectively. If one chooses vectors from the same p-type, then $p_a = p_b = p$ and

$$MAC_{a,b} = \frac{r^2}{p^2}, \tag{7}$$

Since the v_p term is dependent on the $v_1 ... v_{p-1}$ terms, the number of possible repeated terms is $p - 1$. Thus, if $r > p - 1$, it is not possible to form a complete basis from just this one p-type.

Postulate: $r = p - 1$

Proof: For a given n and p, the number of unique indices for the v_i entry is less than or equal to $\lfloor \frac{n-p}{2} \rfloor + 1$ since $v_i \leq v_p$. To form an n vector basis requires $n\,(p-1)$ total entries. There are two consequences of this limit. First, it is not possible for a basis of n vectors to have all unique indices for a given v_i since $n > \lfloor \frac{n-p}{2} \rfloor + 1$. Thus $r \geq 1$ for $p \geq 2$.

REFERENCES