OCTONION MULTIPLICATION AND 7-CUBE VERTICES

DONALD CHESLEY
STAVWAY NUMBER LABS

Abstract. For some dimensions D, the unit D-cube's set of vertices V_D can be partitioned into two disjoint subsets B_D (the "Basis") and N_D (the "Neighbors"), such that every $b \in B_D$ has D "nearest neighbors" one unit away, all in N_D, and every $n \in N_D$ has exactly one nearest neighbor in B_D and $D-1$ nearest neighbors in N_D. A necessary condition for such a partition is $D = 2^k - 1$. Equivalently in binary number representation, only if $D = 2^k - 1$ for some k can there be a subset $B \subset S = \{0, 1, ..., 2^D - 1\}$ such that any $s \in S - B$ is exactly one bit different from exactly one $b \in B$.

Each representation of the octonions arranges the seven imaginary unit elements into seven triads, with no two distinct triads having a pair of element in common. There is a natural mapping between the 30 distinct such sets of triads and the 30 distinct versions of B_7 which contain the vertex (0,0,0,0,0,0,0). Assigning a chirality to each triad of a given octonion representation then reveals that not all 128 possible chirality assignments result in a normed division algebra. In fact, for each of the 30 possible ways of grouping the elements, each of 16 chirality assignments (again corresponding to a B_7) gives a distinct representation of the octonions for a total of 480 representations, and each of the other 112 (corresponding to N_7) gives a distinct representation of the twisted octonion algebra.

1. Definitions and Notation for Any Dimension

Let V_D be the set of vertices of the unit D-dimensional cube, and choose coordinate axes so that the vertices are of form $(x_1, x_2, ..., x_D)$ with each $x_i \in \{0, 1\}$. Two elements $v, w \in V_D$ are "nearest neighbors" (represented as $v \leftrightarrow w$) iff they are unit distance apart, where distance squared d^2 is calculated as the usual Euclidean metric in $\mathbb{R}^D$:

$$d^2(v, w) = \sum_{j=1}^{D} (v_j - w_j)^2. \tag{1}$$

1.1. **XOR (Exclusive OR) and Distance.** Because each coordinate's value is 0 (mappable to False) or 1 (mappable to True), the operation XOR (0 XOR 0 = 0; 1 XOR 1 = 0; 0 XOR 1 = 1; 1 XOR 0 = 1, the truth table for the logic operation "exclusive OR") can be adapted to simplify distance calculation. For each j, $(v_j - w_j)^2 = v_j$ XOR w_j, hence $d^2(v, w) = \sum_{j=1}^{D}(v_j \text{ XOR } w_j)$, so $d^2(v, w) = m$ iff the coordinate representations of v and w differ in exactly m positions. It follows immediately that v has D nearest neighbors, each obtained by changing exactly one of v's D coordinate values; and that $\bar{v}$ (v with all coordinates changed) gives $d^2(v, \bar{v}) = D$.

Date: September 7, 2020.

1.2. **Partitioning V_D by Distance.** For any $v \in V_D$, define (mnemonic: "F" for "Far") $F_D^{(j)}(v) = \{w \in V_D : d^2(w,v) = j\}$. Since $w \in V_D \Rightarrow 0 \le d^2(v,w) \le D$, it follows that $V_D = \cup_{i=0}^{D} F_D^{(i)}(v)$. Moreover, if $w \in F_D^{(i)}(v) \cap F_D^{(j)}(v)$, then by definition $d^2(v,w) = i$ and $d^2(v,w) = j$, so $i \neq j \Rightarrow F_D^{(i)}(v) \cap F_D^{(j)}(v) = \emptyset$.

Since $w \in F_D^{(i)}(v) \Leftrightarrow d^2(v,w) = i$, and $d^2(v,w) = i$ iff w differs from v in i of D coordinates, the count of elements in $F_D^{(i)}$ is the number of ways of choosing i from D:

$$|F_D^{(i)}(v)| = \frac{D!}{(D-i)!i!} = \binom{D}{i} \tag{2}$$

1.3. **V_D as a Group with XOR as its Product.** For any D, let ς_D be the D-dimensional zero vector. V_D forms a commutative group, with group product vw, defined by:

$$vw \equiv (v_1 \ XOR \ w_1, v_2 \ XOR \ w_2, ...v_D \ XOR \ w_D), \tag{3}$$

having unit element ς_D:

$$\varsigma_D v = v\varsigma_D = v \tag{4}$$

and with every element its own inverse:

$$vv = \varsigma_D. \tag{5}$$

XOR acts associatively on individual components, and any $x \in V_D$ with components x_i satisfies (v_i XOR x_i) XOR (w_i XOR x_i) = v_i XOR w_i, hence

$$d^2(xv, xw) = d^2(v,w), \tag{6}$$

For any subset $S = \{s_1, s_2, ...s_m\} \subseteq V_D$, and for any $v \in V_D$, let vS be the set $\{vs_1, vs_2, ..., vs_m\}$. Then for $1 \le i, j \le m$, $d^2(vs_i, vs_j) = d^2(s_i, s_j)$.

1.4. **Subgroups of V_D.** Equations (3)-(5) above describe the group properties of V_D with XOR as the group operation. Since $|V_D| = 2^D$, it has subgroups of order 2^n for $0 \le n \le D$.

Recall that $\bar{v}$ is the "complement" of v, with all its coordinates inverted (0 replaced by 1, and 1 replaced by 0), so $\bar{\varsigma}_D$ is the D-dimensional vector with all coordinates equal to 1; then $\bar{\varsigma}_D v = v\bar{\varsigma}_D = \bar{v}$ and $v\bar{v} = \bar{v}v = \bar{\varsigma}_D$; hence, for any subgroup S of V_D, if $v \in S$ and $\bar{v} \in S$, then $\bar{\varsigma}_D \in S$, hence for any $w \in S$, $\bar{w} \in S$. Subgroups not containing $\bar{\varsigma}_D$ exist for all orders $< D$; subgroups containing $\bar{\varsigma}_D$ exist for order > 0 and $\le D$.

- The unique subgroup of order 2^0 is $\{\varsigma_D\}$;
- Since $vv = \varsigma_D$ for any $v \in V_D$, all order 2 subgroups are of the form $\{\varsigma_D, v\}$, and any $v \in V_D$ generates such a group; a special case of interest is $\{\varsigma_D, \bar{\varsigma}_D\}$;
- if S is a subgroup of V_D order 2^n and $v \in V_D, v \notin S$, then vS is a nontrivial coset of S, and $S \cup vS$ is a subgroup of V_D of order 2^{n+1};

Geometrically, v and $\bar{v}$ are opposite endpoints of a maximal diagonal of the D-cube. A subgroup $S \ni \bar{\varsigma}_D$, and all of S's cosets, contain all maximal diagonals of their elements.

2. Partitionable Dimensions

Assume it is possible to partition V_D into two disjoint subsets B_D (the "Basis"), and N_D (the "Neighbors"), such that each $b \in B$ has all D of its nearest neighbors be in N, and each $n \in N$ has exactly one nearest neighbor in B, *i.e.*:

$$V_D = B_D \cup N_D, B_D \cap N_D = \emptyset \tag{7}$$

$$b_1, b_2 \in B_D \Rightarrow\Leftarrow b_1 \leftrightarrow b_2 \tag{8}$$

$$n \in N_D \Rightarrow \exists! b \in B_D : n \leftrightarrow b \tag{9}$$

For $v, w \in V_D$ with $d^2(v, w) = 2$, there are just two coordinates in which v, w differ, so there exist two distinct elements $x, y \in V_D$ differing by one coordinate from each of v, w; thus (8) and (9) above imply that at least one of $v, w \notin B_D$, *i.e.* $v, w \in B_D \Rightarrow d^2(v, w) > 2$.

A counting analysis easily reveals a necessary condition on dimension D. To satisfy the partitioning requirements above, every $b \in B_D$ must have D nearest neighbors in N_D, and every $n \in N_D$ must have exactly one nearest neighbor $\in B_D$, so defining $\beta_D \equiv |B_D|$, $\nu_D \equiv |N_D|$:

$$\beta_D D = \nu_D \tag{10}$$

$$\beta_D + \nu_D = 2^D \tag{11}$$

$$\Rightarrow \beta_D(D + 1) = 2^D \tag{12}$$

and thus there is a $k \leq D$ such that $\beta_D = 2^{D-k}$ and $D = 2^k - 1$.

If the D-cube has a partition $V_D = B_D \cup N_D$ of the desired type, $B_D \neq \emptyset$, so $\exists b \in B_D$. Let $B_D^{(i)}(b) = B_D \cap F_D^{(i)}(b)$ and $N_D^{(i)}(b) = N_D \cap F_D^{(i)}(b)$, with $\beta_D = |B_D|$, $\nu_D = |N_D|$, $\beta_D^{(i)}(b) = |B_D^{(i)}(b)|$, and $\nu_D^{(i)}(b) = |N_D^{(i)}(b)|$.

Nearest neighbors of $n \in N_D^{(i)}(b)$ must be either in $F_D^{(i-1)}(b)$ or $F_D^{(i+1)}(b)$, inducing the convenient partitioning $N_D^{(i)}(b) = N_{D_B}^{(i)}(b) \cup N_{D^B}^{(i)}(b)$ (mnemonic "lower B" in D_B denotes "lower superscript value" in $B_D^{(i-1)}$; similarly for "upper" D^B and $B_D^{(i+1)}$):

$$N_{D_B}^{(i)}(b) = \{n \in N_D^{(i)}(b) : (\exists b' \in B_D^{(i-1)}(b) : b' \leftrightarrow n)\}, |N_{D_B}^{(i)}(b)| = \nu_{D_B}^{(i)}(b); \tag{13}$$

$$N_{D^B}^{(i)}(b) = \{n \in N_D^{(i)}(b) : (\exists b' \in B_D^{(i+1)}(b) : b' \leftrightarrow n)\}, |N_{D^B}^{(i)}(b)| = \nu_{D^B(b)}^{(i)}; \tag{14}$$

and (else some n would have 2 nearest neighbors in B):

$$N_{D_B}^{(i)}(b) \cap N_{D^B}^{(i)}(b) = \emptyset \tag{15}$$

For any $b \in B_D$, $\beta_D^{(0)}(b) = 1$ and $\nu_D^{(0)}(b) = 0$. At distance squared $d^2(b, v) = i$ from b there are $|F_D^{(i)}(b)| = \binom{D}{i}$ elements $v \in V_D$ with each such v having i coordinates different from the corresponding coordinates of b, and having $D - i$ coordinates the same. Changing any one of those different (same) coordinates of v will result in an element $v' \in F^{(i-1)}_{D^B}(b)$ (or $v' \in F^{(i+1)}_{D_B}(b)$ respectively). If $v \in B_D$ then $v' \in N_D$. Thus, for $0 < i \leq D$:

$$\beta^{(i)}_D(b) = \nu^{(i-1)}_{D^B}(b)/i \tag{16}$$

$$\nu^{(i)}_D(b) = \binom{D}{i} - \beta^{(i)}_D(b) \tag{17}$$

$$\nu^{(i)}_{D_B}(b) = (D - i + 1)\beta^{(i-1)}_D(b) \tag{18}$$

$$\nu^{(i)}_{D^B}(b) = \nu^{(i)}_D(b) - \nu^{(i)}_{D_B}(b). \tag{19}$$

These necessary conditions on the distances between pairs of elements in B_D assist the search for partitions satisfying the required conditions (as will be seen for B_7).

If S satisfies the conditions (16)-(19), vS does as well (note that $D = 2^k - 1$, and $|S| = \beta_D = 2^{D-k}$ are then necessary conditions). Since $vv = \varsigma_D$, $v \in S \Rightarrow \varsigma_D \in vS$. Hence for any B_D satisfying the partition requirements for a Basis, either $\varsigma_D \in B_D$, or for any $b \in B_D$, bB_D is also a Basis that satisfies the partitioning requirements and contains ς_D. As will be seen, having ς_D as an element in a Basis simplifes the construction of concrete examples of $V_7 = B_7 \cup N_7$.

3. The 0-, 1-, 3-, and 7-cubes

The 0-cube is just a point v_0, and $B_0 = V_0 = \{v_0\}$, $N_0 = \emptyset$ satisfies the desired conditions. Similarly, the unit 1-cube is two points on the number line, v_0 at 0 and v_1 at 1, with B_1 containing one of these points, and N_1 containing the other. The 2-cube (*i.e.* the square), cannot be so partitioned (try drawing it!), but the 3-cube can, with B_3 comprising two points at opposite ends of a major diagonal (of length $\sqrt{3}$ for a unit 3-cube).

For $D = 7$, application of the counting conditions (16)-(19) above, starting from any $b \in B_7$, gives:

$$\beta^{(0)}_7(b) = \beta^{(7)}_7(b) = 1, \text{ from which follows } b \in B_7 \Leftrightarrow \bar{b} \in B_7;$$
$$\beta^{(3)}_7(b) = \beta^{(4)}_7(b) = 7, \text{ implying } v \in B^{(3)}_7(b) \Leftrightarrow \bar{v} \in B^{(4)}_7(b);$$
$$\beta^{(1)}_7(b) = \beta^{(2)}_7(b) = \beta^{(5)}_7(b) = \beta^{(6)}_7(b) = 0.$$

so $b, b' \in B_7 \Rightarrow d^2(b, b') = 3, 4,$ or 7. The counts of elements not in B_7 are given by:

$$\nu^{(0)}_7(b) = \nu^{(7)}_7(b) = 0; \nu^{(1)}_7(b) = \nu^{(6)}_7(b) = 7; \nu^{(2)}_7(b) = \nu^{(5)}_7(b) = 21; \nu^{(3)}_7(b) = \nu^{(4)}_7(b) = 28.$$

For any $b \in B_7$, the set $bB_7 \ni \varsigma_7$ also satisfies the counts above and preserves distances among the elements of the set, and $v \in F^{(i)}_D(\varsigma_7) \Leftrightarrow d^2(\varsigma_7, v) = i$, that is, v has exactly i coordinates equal to 1. For $v, v' \in F^{(3)}_7(\varsigma_7)$, $d^2(v, v') \in \{2, 4, 6\}$, and by the counting in $(16) - (19)$, only $d^2(v, v') = 4$ is permitted for $D = 7$.

4. Constructing All Partitions of V_7

To construct a concrete example of B_7, assign $\varsigma_7 \in B_7^{(0)}$, and find seven elements $b_i \in F_7^{(3)}(\varsigma_7)$ such that $d^2(b_i, b_j) = 4$, for all $1 \leq i, j \leq 7, i \neq j$. Pick an arbitrary element of $F_7^{(3)}(\varsigma_7)$ to be b_1. Any vector w having three coordinates equal to 1 and satisfying $d^2(b_1, w) = 4$ must be obtained from b_1 by swapping two of b_1's 1-valued coordinates with two of its 0-valued coordinates. There are three ways of choosing two 1-coordinates to be swapped (leaving one of the original 1-valued coordinates in place), and six ways of swapping those two 1-valued coordinates into two of the four 0-valued coordinates. Viewing a b_i vector obtained by such swapping as the vector sum of an "enhanced" vector (containing the two 1-valued coordinates in the positions to which they are swapped; left column below), and a "depleted" vector (b_1 minus the two 1-valued coordinates being swapped; right column); for example, let $b_1 = (0{,}0{,}0{,}0{,}1{,}1{,}1)$:

```
  ENHANCED          DEPLETED
(0,0,1,1,0,0,0)   (0,0,0,0,0,0,1)
(1,1,0,0,0,0,0)   (0,0,0,0,0,1,0)
(0,1,0,1,0,0,0)   (0,0,0,0,1,0,0)
(1,0,1,0,0,0,0)
(0,1,1,0,0,0,0)
(1,0,0,1,0,0,0)
```

For a vector L from the left column and a vector R from the right, $L+R \in F_7^{(3)}(\varsigma_7)$ (having three coordinates equal to 1), and $d^2(L+R, b_1) = 4$. However, $d^2(L+R, L+R') = 2$ for any R' from the right column where $R' \neq R$. Furthermore, for $L' \neq L$, $d^2(L+R, L'+R) = 4$ iff $L + L'$ has exactly four coordinates with value 1. From these constraints on combining L's with R's, it follows that for a given choice of $b_1 \in F_7^{(3)}(\varsigma_7)$ there are six distinct $B_7^{(3)}(\varsigma_7)$'s. For a choice of b_1 other than (0,0,0,0,1,1,1), the logic is the same, and the patterns for populating the coordinates of the L's and R's with 1's are determined by which three coordinates of b_1 are 1's; those coordinates must be 0's in every L, and each R will have one of these coordinates 1 and the other two 0.

For a given $B_7^{(3)}(\varsigma_7)$, the construction is completed by noting that since $b \in B_7 \Leftrightarrow \bar{b} \in B_7$, it follows that $B_7^{(4)}(\varsigma_7) = \{\bar{b_1}, \bar{b_2}, \bar{b_3}, \bar{b_4}, \bar{b_5}, \bar{b_6}, \bar{b_7}\}$, and $B_7^{(7)}(\varsigma_7) = \{\bar{\varsigma_7}\}$. As a concrete example, let b_1 be (0,0,0,0,1,1,1) as above with the pairings of L's with R's apparent by inspection. The first column is $B_7^{(3)}(\varsigma_7)$, and the second column is $B_7^{(4)}(\varsigma_7)$):

```
(0,0,0,0,1,1,1)   (1,1,1,1,0,0,0)
(0,0,1,1,0,0,1)   (1,1,0,0,1,1,0)
(1,1,0,0,0,0,1)   (0,0,1,1,1,1,0)
(0,1,0,1,0,1,0)   (1,0,1,0,1,0,1)
(1,0,1,0,0,1,0)   (0,1,0,1,1,0,1)
(0,1,1,0,1,0,0)   (1,0,0,1,0,1,1)
(1,0,0,1,1,0,0)   (0,1,1,0,0,1,1)
```

Any two elements $l_i, l_j \in B_7^{(3)}(\varsigma_7), i \neq j$ (left column) can be seen by inspection to satisfy $d^2(l_i, l_j) = 4$; similarly for any two $r_i, r_j \in B_7^{(4)}(\varsigma_7)$ (right column); $d^2(l_i, r_i) = 7$; and $d^2(l_i, r_j) = 3$ $(i \neq j)$.

Each of the $|F_7^{(3)}| = 35$ v's in $F_7^{(3)}(\varsigma_7)$ has six distinct versions of $B_7^{(3)}(\varsigma_7)$ containing it, and each distinct $B_7^{(3)}(\varsigma_7)$ uniquely determines a B_7. Since each distinct $B_7^{(3)}(\varsigma_7)$ is associated with $|B_7^{(3)}| = 7$ elements it contains, the total number of distinct partitions of V_7 in which B_7 contains ς_7 is $\frac{35\times6}{7} = 30$. Examination of the example above shows that it's no coincidence that 30 is also the number of ways of constructing the quaternionic triads contained in a representation of the octonions. Interpreting (0,0,0,0,1,1,1) as $e_1 + e_2 + e_3$, (0,0,1,1,0,0,1) as $e_1 + e_4 + e_5$), and so on, shows that the example $B_7^{(3)}(\varsigma_7)$ shown above represents the seven quaternionic triads in a particular representation of the octonions. The grouping of the orthonormal imaginary units of the octonions into quaternionic triads follows the basic rule of Steiner triple systems that any pair of elements has a unique associated third element, and inspection shows that any pair of 1-valued coordinates occurs in only one of the vectors in the sample $B_7^{(3)}(\varsigma_7)$ above, with that vector's third 1-valued coordinate indicating the "uniquely associated third element".

Each $B_7(\varsigma_7)$ is closed under the action of XOR and hence is a subgroup of order 16, of the type which contains $\bar{\varsigma}_7$. There are $|V_7|/|B_7| = 128/16 = 8$ distinct cosets for each of the 30 distinct $B_7(\varsigma_7)$s, any one of which is also a valid B_7 Basis, but only those containing ς_7 exhibit the close connection to representations of the octonions as described above.

5. The Polytope with Vertices $\in B_7$

For each $x \in V_7$, the associated distance-preserving operation can be used to examine the geometric structure of the vertices in a given instance of B_7, and to generate other instances comprising a different subset of V_7 (or if $x \in B_7$, the same subset of V_7, since then $xB_7 = B_7$).

To be investigated and/or described:

(1) $\forall D = 2^k - 1, \quad b \in B_D \Rightarrow \overline{b} \in B_D$ where $\overline{v}$ is the complement of v, i.e. 0-valued coordinates become 1, and 1-valued coordinates become 0;
(2) no alternate version with vertices $\sqrt{6}$ units apart (though there are in D=15)
(3) B_7 is 7-dim, as determined by Gram-Schmidt basis generation:
starting with vertices {19,2a,34,4b,52,61,78}, get 7 orthogonal vectors:
(0,0,1,1,0,0,1), $\frac{1}{3}$(0,3,-1,2,0,3,-1), $\frac{1}{4}$(0,3,3,-2,4,-1,-1), $\frac{1}{5}$(5,-1,-1,-1,2,2,2),
$\frac{1}{4}$(1,-1,3,-1,-2,2,-2), $\frac{1}{3}$(1,2,0,-1,-2,-1,1), $\frac{1}{2}$(1,0,0,1,0,-1,-1)
(4) all variants (choices of $b \in B_7^{(3)}$): 30 16-dim subgroups, plus all cosets thereof of form $b'B_7, b' \notin B_7$
(5) What symmetries? certainly permutation of order of coordinates; G_2 Lie algebra?? as suggested by connections with octonion triad grouping, and with chirality
(6) Edges are length $\sqrt{3}$, $\sqrt{4}$; internal diagonals are length $\sqrt{7}$

(7) is it convex?
(8) Faces are triangles with sides $\sqrt{3}$, $\sqrt{4}$, $\sqrt{3}$ (how many?)
(9) Any 3 $b \in B_7$, if not the vertices of a face, form a triangle w sides $\sqrt{4}$, $\sqrt{4}$, $\sqrt{4}$ or $\sqrt{3}$, $\sqrt{4}$, $\sqrt{7}$
(10) 3-D intersections tetrahedron w base edges $\sqrt{4}$, slope edges $\sqrt{3}$ - count

Choosing $B_7 \ni \varsigma_7$, and using hexadecimal to represent a 7-tuple of 0's and 1's regarded as a bit string (*e.g.* (1,0,1,1,1,0,1) $\Leftrightarrow$ 1011101 $\Leftrightarrow$ 5d), enables the compact notation $F_7^{(3)}(\varsigma_7) = \{07, 0b, 0d, 0e, 13, 15, 16, 19, 1a,$
$1c, 23, 25, 26, 29, 2a, 2c, 31, 32, 34, 38, 43, 45, 46, 49, 4a, 4c, 51, 52, 54, 58, 61, 62, 64, 68, 70\}$ (*i.e.* all numbers < 128 with 3 bits set).