# Regular Simplices Inscribed into the Cube and Exhibiting a Group Structure

Walter Wenzel[1]
Fakultät für Mathematik, Technische Universität Chemnitz, D–09107 Chemnitz, Germany
email: walter@mathematik.tu-chemnitz.de

**Abstract**

For $n \in \mathbb{N}$, we interpret the vertex set $W_n$ of the $n$-cube as a vector space over the field $\mathbb{F}_2$ and prove that a regular $n$-simplex can be inscribed into the $n$-cube such that its vertices constitute a subgroup of $W_n$ if and only if $n+1$ is a power of 2. Furthermore, a connection to the theory of Hamming Codes will be established.

## § 1 Introduction

Many mathematicians have considered problems as follows:

(I) Which convex polytopes $P \subseteq \mathbb{R}^n$ with regularity properties can be embedded into $\mathbb{R}^n$ via a similarity transformation such that every vertex of $P$ becomes a lattice point in $\mathbb{Z}^n$?

(II) Which regular polytopes $P$ can be inscribed into a given regular polytope $P_0$ such that every vertex of $P$ is also a vertex of $P_0$?

In 1937, I. J. Schoenberg [14] had solved Problem (I) in case $P$ is a regular simplex. By making use of quadratic forms, he determined all dimensions $n$ for which there exist regular $n$-simplices exhibiting only integer coordinates. Almost simultaneously, H. Hadwiger settled the same problem in [4] for even $n$. See also [12], where the equivalence of this problem to the existence of Hadamard matrices is settled. Later on, many authors examined the problem for which dimensions $n$ a regular $n$-simplex can be inscribed *faithfully* into the $n$-cube, that means, each vertex of the simplex is also a vertex of the cube; see, for instance, [6], [5], [11], [3], [15], as well as the

[1] temporary address:
Max-Planck-Institute for Mathematics in Sciences, Inselstr. 22-26, D–04103 Leipzig, Germany

survey [9]. In particular, A. I. Medjanik has proved in [11] that the condition $n \equiv 3 \bmod 4$ is necessary, and, up to now, no counter-example to the assumption that this condition also suffices is known.

Several generalizations, concerning the above mentioned Problem (II), are studied in [7].

In the present note, we study the following question: For which dimensions $n$ is it possible to inscribe a regular $n$-simplex $S$ into the $n$-cube, whose vertex set $W_n$ is identified with the vector space $\mathbb{F}_2^n$ in a canonical way, such that the vertices of $S$ constitute a subgroup of $(\mathbb{F}_2^n, +)$?

In Theorem 2.2, it is proved that this is the case if and only if $n+1$ is a power of 2. Moreover, exactly in this case there exist $\frac{1}{n+1} \cdot 2^n$ regular $n$-simplices whose vertex sets constitute a disjoint covering of $W_n$.

Moreover, in Section 3 we prove that a linear subspace $U$ of the vector space $\mathbb{F}_2^n$ is – considered as a subset of $W_n$ – the set of vertices of a regular simplex of dimension $n$ if and only if the orthogonal space $U^\perp$ is a Hamming Code of dimension $n - \log_2(n+1)$ over the field $\mathbb{F}_2$.

For a recent contribution concerning coverings and packings of the $n$-cube by socalled rectangular simplices see [10].

## § 2 Regular simplices with a group structure

For a convex polytope $P \subseteq \mathbb{R}^n$, let $V(P)$ denote the vertex set of $P$. Furthermore, put

$$\text{(2.1 a)} \quad C_n := [0,1]^n ,$$

$$\text{(2.1 b)} \quad W_n := \{0,1\}^n = V(C_n) .$$

Let "$\oplus$" denote addition in $W_n$ modulo 2; thus $(W_n, \oplus)$ is a group which is canonically isomorphic to $(\mathbb{F}_2^n, +)$. Since we consider $W_n$ as a subset of $\mathbb{R}^n$, we prefer to write "$\oplus$" rather than "+".

**Remark 2.1:** If $x = (x_1, \ldots, x_n) \in W_n$ and $x_{i_j} = 1$ for exactly $k$ indices $1 \le i_1 < \ldots < i_k \le n$, then the map $f_x : W_n \to W_n$, defined by $f_x(w) :=$

$x \oplus w$, is the restriction of some congruence map defined on $\mathbb{R}^n$; namely we have

$$f_x(w) = (s_{i_1} \circ \ldots \circ s_{i_k})(w) \quad \text{for } w \in W_n ,$$

where $s_\nu$, $1 \leq \nu \leq n$, denotes the reflection at the affine hyperplane

$$H_\nu := \{(t_1, \ldots, t_n) \in \mathbb{R}^n | t_\nu = \frac{1}{2}\} .$$

This means: For every subset $V_0 \subseteq W_n$ the sets conv $(V_0)$ and conv $(f_x(V_0))$ are congruent, where "conv" means convex hull. □

In what follows, a (regular) simplex $S \subseteq \mathbb{R}^n$ will always mean the convex hull of an affinely independent set; in particular, one has

$$\text{conv } (V(S)) = S .$$

We can now prove

**Theorem 2.2:** For $n \geq 3$, the following three statements are equivalent:

(i) $(W_n, \oplus)$ contains some subgroup $U$ such that conv $(U)$ is a regular simplex of dimension $n$.

(ii) For $m := \frac{1}{n+1} \cdot 2^n$ one has

$$(2.2) \qquad W_n = V(S_1) \dot{\cup} \ldots \dot{\cup} V(S_m)$$

for certain regular simplices $S_1, \ldots, S_m$ of dimension $n$.

(iii) $n + 1$ is some power of 2.

**Proof:** (i) $\Longrightarrow$ (ii):
By (i), we have $|U| = n + 1$. Let $N_1, \ldots, N_m$ denote the cosets of $U$ in $W_n$, and put $S_i :=$ conv $(N_i)$ for $1 \leq i \leq m = \frac{1}{n+1} \cdot 2^n$. Then Remark 2.1 implies that $S_1, \ldots, S_m$ are regular $n$-dimensional simplices, and we have

$$W_n = N_1 \dot{\cup} \ldots \dot{\cup} N_m = V(S_1) \dot{\cup} \ldots \dot{\cup} V(S_m) .$$

(ii) $\Longrightarrow$ (iii) is trivial.

(iii) $\Longrightarrow$ (i):
We proceed by induction on $\log_2(n+1)$. For $n = 3$ put

$$U = U_3 = \{(0,0,0),(1,1,0),(1,0,1),(0,1,1)\}\ .$$

In particular, any two distinct vertices in $U_3$ have Hamming distance 2.

Now assume that $n \geq 3$ satisfies $\log_2(n+1) \in \mathbb{N}$, and that

$$U = U_n = \{v_1,\dots,v_{n+1}\} \subseteq W_n$$

satisfies (i) for $n$, where $v_1 = (0,\dots,0)$ and any two distinct vertices in $U_n$ have Hamming distance $\frac{n+1}{2}$. Write

$$\text{(2.3 a)} \qquad v_i = (v_{i1},\dots,v_{in}) \text{ for } 1 \leq i \leq n+1$$

and define $w_1,\dots,w_{n+1},w_{n+2},\dots,w_{2n+2} \in W_{2n+1}$ by

$$\text{(2.3 b)} \qquad w_i := (v_{i1},v_{i1},v_{i2},v_{i2},\dots,v_{in},v_{in},0) \text{ for } 1 \leq i \leq n+1\,,$$

$$\text{(2.3 c)} \qquad w_{n+2} := (1,0,1,0,1,\dots,1,0,1)\,,$$

$$\text{(2.3 d)} \qquad w_{n+1+i} := w_i \oplus w_{n+2} \text{ for } 2 \leq i \leq n+1\,.$$

By construction,

$$\text{(2.4)} \qquad U_{2n+1} := \{w_1,\dots,w_{n+1},w_{n+2},\dots,w_{2n+2}\}$$

is a subgroup of $(W_{2n+1},\oplus)$ with $w_1 = (0,\dots,0)$, and any $w_i, w_j$, $1 \leq i < j \leq 2n+2$, have Hamming distance $n+1$ and Euclidean distance $\sqrt{n+1}$. Since $|U_{2n+1}| = 2n+2$, we see that conv $(U_{2n+1})$ is a regular $(2n+1)$-dimensional simplex as claimed. □

**Remark 2.3:** The step "(iii) $\Rightarrow$ (i)" in the last proof can also be achieved in terms of Hadamard matrices. However, the above construction is more direct.

## § 3 A Connection to the Theory of Hamming Codes

In this section, we identify $W_n$ with the vector space $\mathbb{F}_2^n = (\mathbb{Z}/2\mathbb{Z})^n$ in the obvious way, but consider the elements of $\mathbb{F}_2^n$ as columns. For a linear subspace $U$ of $\mathbb{F}_2^n$ we write as usual

$$(3.1) \qquad U^{\perp} := \{v \in \mathbb{F}_2^n | w^{\top} \cdot v = 0 \text{ for all } w \in U\}.$$

Note that $\mathbb{F}_2^n$ contains a Hamming Code – that is a 1-perfect error correcting code – if and only if $n+1$ is some power of 2. (For the theory of Hamming Codes cf., for example, [1], (Section 12.4), [2], (Section 11.1), or [13], (Section 2.2).) Thus, the existence of Hamming Codes in $\mathbb{F}_2^n$ is equivalent to all of the statements in Theorem 2.2. In what follows, assume $n+1 = 2^r$ for some $r \in \mathbb{N}$. Now we prove the following stronger connection between regular simplices and Hamming Codes.

**Theorem 3.1:** For a linear subspace $U$ of $\mathbb{F}_2^n$, the following two statements are equivalent:

(i) $U$ is – considered as a subgroup of $(W_n, \oplus)$ – the set of vertices of a regular simplex $S =$ conv $(U)$ of dimension $n$.

(ii) $U^{\perp}$ is a Hamming Code of dimension $n - r$.

**Proof:** First of all, note that the dimension $n$ of $S$ in (i) is considered over the field $\mathbb{R}$ of real numbers, while the dimension $n - r$ of $U^{\perp}$ in (ii) is considered over the field $\mathbb{F}_2$.

(i) $\Longrightarrow$ (ii):
Write $U = \{\mathbf{u}_1, \ldots, \mathbf{u}_{n+1}\}$ as well as

$$\mathbf{u}_i = (u_{i1}, \ldots, u_{in})^{\top} \quad \text{for } 1 \leq i \leq n+1.$$

Choose some linear base $B$ of the $\mathbb{F}_2$-vector space $U$. Since $|U| = n+1 = 2^r$, one has $|B| = r$, say $B = \{\mathbf{u}_1, \ldots, \mathbf{u}_r\}$. Consider the matrix

$$(3.2) \qquad M := \begin{pmatrix} \mathbf{u}_1^{\top} \\ \vdots \\ \mathbf{u}_r^{\top} \end{pmatrix} = (u_{ij})_{1 \leq i \leq r, 1 \leq j \leq n}$$

as well as the $\mathbb{F}_2$-vector space

$$(3.3) \qquad C := U^{\perp} = \{(c_1, \ldots, c_n)^{\top} \in \mathbb{F}_2^n \,|\, M \cdot (c_1, \ldots, c_n)^{\top} = 0\}.$$

The matrix $M$ has rank $r$; thus the subspace $C$ of $\mathbb{F}_2^n$ has dimension $n - r$. Since conv $(U)$ is a nondegenerate simplex in $\mathbb{R}^n$, $B$ is neither contained in a hyperplane

$$\left\{(t_1, \ldots, t_n)^{\top} \in \mathbb{F}_2^n | t_\nu = 0\right\} \text{ for some } \nu \text{ with } 1 \le \nu \le n,$$

nor in a hyperplane

$$\left\{(t_1, \ldots, t_n)^{\top} \in \mathbb{F}_2^n | t_\nu = t_\mu\right\} \text{ for certain } \nu, \mu \text{ with } 1 \le \nu < \mu \le n.$$

This means that any two columns of $M$ are linearly independent over $\mathbb{F}_2$. Thus $M$ must exhibit any column vector of $\mathbb{F}_2^r \setminus \{0\}$ exactly once, because $M$ contains exactly $n = 2^r - 1$ columns. Therefore, by the theory of Hamming Codes, any two different vectors of $C = U^{\perp}$ have Hamming distance at least 3, and $C$ is a Hamming Code in $\mathbb{F}_2^n$.

"$\Longleftarrow$":
Assume $C = U^{\perp}$ is a Hamming Code of dimension $n - r = 2^r - r - 1$. According to Theorem 2.2, choose some linear subspace $U_0 \subseteq \mathbb{F}_2^n \cong W_n$ such that $S =$ conv $(U_0)$ is a regular simplex of dimension $n$. By the first part of this proof, $U_0^{\perp}$ is a Hamming Code of dimension $n - r$. There exists some permutation $\pi \in S_n$ such that the two Hamming Codes $U^{\perp}$ and $U_0^{\perp}$ in $\mathbb{F}_2^n$ satisfy the relation

$$U^{\perp} = \left\{(t_{\pi(1)}, \ldots, t_{\pi(n)}) | (t_1, \ldots, t_n) \in U_0^{\perp}\right\}.$$

Thus we have also

$$U = \left\{\left(t_{\pi(1)}, \ldots, t_{\pi(n)}\right) | (t_1, \ldots, t_n) \in U_0\right\}.$$

Therefore, $U = C^{\perp}$ satisfies (i), because $U_0$ does. □

**Remark 3.2:** It is already mentioned in [8], Chapter 1, Section 9 – neither with a proof, nor with a reference – that the codewords of the dual of a binary Hamming Code form a regular simplex and that this dual code is therefore also called a Simplex Code. Nothing is said about the above conclusion "(i) $\Rightarrow$ (ii)".

**Acknowledgement**

The author wishes to thank Eike Hertel and Horst Martini for several discussions concerning the history of the problem of inscribing a regular $n$-simplex faithfully into the $n$-cube.

# References

[1] M. Aigner: *Diskrete Mathematik.* Vieweg, Berlin, 1993.

[2] G. Cohen, I. Honkala, S. Litsyn, and A. Lobstein: *Covering Codes.* Elsevier, Amsterdam, 1997.

[3] V. L. Dol'nikov: *On the Jung constant in $l_1^n$* (Russ.). Mat. Zametki 42 (1987), 519-526; Transl.: Math. Notes 42 (1987), 787-791.

[4] H. Hadwiger: *Über die rationale Lagerung des regulären Simplex.* Math. Z. 42 (1937), 625-628. Verlag von Julius Springer, Berlin W9.

[5] H. Hadwiger: *Ungelöste Probleme Nr. 10.* Elem. Math. 11 (1956), 36-37.

[6] J. D. Jarratt and J. J. Seidel: *A note on the equivalence of the problem of embedding a regular N-simplex in the N-dimensional hypercubic lattice to a certain integral matrix completion problem.* Indian J. Math. 27 (1985), 57-62.

[7] W. F. Kibble: *Regular polytopes inscribed in other regular polytopes.* Math. Student 17 (1949), 26-31.

[8] F. J. Mac Williams, N. J. A. Sloane: *The Theory of Error-Correcting Codes.* North-Holland Mathematical Library, Amsterdam, London, New York, Tokyo 1993.

[9] H. Martini: *A hierarchical classification of Euclidean polytopes with regularity properties, in: Polytopes-Abstract, Convex and Computational.* NATO ASI Series C, 440, T. Bisztriczky, P. Mc Mullen, R. Schneider and A. Ivić Weiss (eds.). Kluwer Academic Publishers, Dordrecht (1994), 71-96.

[10] H. Martini and W. Wenzel: *Covering and packing problems in lattices associated with the n-cube.* European J. Combin. 23 (2002), 63-75.

[11] A. I. Medjanik: *A regular simplex inscribed in the cube* (Russ.). Ukrain. Geometr. Sb. Vyp. 13 (1973), 109-112.

[12] M. J. Pelling: *Regular simplices with rational vertices.* Bull. London Math. Soc. 9 (1977), 199-200.

[13] V. Pless: *Introduction to the theory of error-correcting codes.* Interscience Series in Discrete Mathematics, Wiley, New York, 1982.

[14] I. J. Schoenberg: *Regular simplices and quadratic forms.* J. London Math. Soc. 12 (1937), 48-55.

[15] W. Wallis: *Combinatorial Designs.* Monographs and Textbooks in Pure and Applied Mathematics, 118. Marcel Dekker, Inc., New York and Basel, 1988.