MINIMUM DISTANCE AND DECODING OF COXETER CODES

ALEXANDER BARG, QËNDRIM R. GASHI, AND TIANYUAN XU

Abstract. A binary Coxeter code associated with a finite Coxeter system (W, S) is an $\mathbb{F}_2$-linear span of indicators of standard cosets of a fixed rank. Coxeter codes, introduced in a recent paper by N. Coble and A. Barg, are a generalization of Reed–Muller codes which arise when $W = \mathbb{Z}_2^m$ is the Coxeter group of type mA_1. In that paper, the authors proposed a conjectural value for the minimum distance of a general Coxeter code. This conjecture is proved in the present work. As a consequence, we obtain a Coxeter-theoretic generalization of Reed's majority-logic decoding algorithm for Reed–Muller codes.

1. Introduction

Let (W, S) be a finite Coxeter system, where W is a finite group with a generating set $S = \{s_1, \ldots, s_m\}$ satisfying the defining relations $(s_i s_j)^{M(i,j)} = 1$ with $M(i,i) = 1$ and $M(i,j) = M(j,i) \geq 2$ for $i \neq j$. A standard (left) coset of rank r in W is a coset of the form wW_I, where $w \in W, I \subseteq S$, and W_I is a standard parabolic subgroup of rank $|I| = r$. We refer to [4] for an introduction to the combinatorics of Coxeter groups.

Recently, Coble and Barg [6] introduced a class of binary linear codes spanned by indicators of standard cosets of W of a fixed rank. Specifically, they defined a *Coxeter code* $\mathsf{C}_W(r)$ of order $r \in \{-1, 0, \ldots, m\}$ to be the $\mathbb{F}_2$-linear span of indicator vectors of the standard cosets of rank $m - r$:

$$\mathsf{C}_W(r) := \operatorname{Span}\{\mathbb{1}_{wW_I} \mid w \in W, I \subseteq S, |I| = m - r\}. \tag{1}$$

The value -1 is included for convenience since it enables one to properly formulate the duality results for Coxeter codes [6, Sec.3]. At the same time, we have $\mathsf{C}_W(-1) = \{0\}$ by definition. The codes in (1) form a direct generalization of a classic family of binary codes known as Reed–Muller codes $RM(r, m)$, which correspond to Coxeter type mA_1, where $S = \{e_1, \ldots, e_m\}$ and $W = \mathbb{Z}_2^m$ is a direct product of m permutation groups on 2 elements, with generators corresponding to the vectors of the standard basis. Reed–Muller codes have been extensively studied in classical coding theory [10, Ch.13–15], [2], [1], and they also give rise to a family of quantum CSS codes with a range of well-understood properties [3].

The Coxeter code $\mathsf{C}_W(r)$ has length $|W|$ by construction, and its dimension is

$$\dim \mathsf{C}_W(r) = \sum_{i=0}^{r} \left\langle {W \atop i} \right\rangle, \tag{2}$$

where the W-Eulerian number $\left\langle {W \atop i} \right\rangle, i \in \{0, \ldots, m\}$ is the count of elements in W with descent number equal to i, [4, Sec.7.2]. For the classical Reed–Muller code $RM(r, m)$, this dimension reduces to the familiar expression $\sum_{i=0}^{r} \binom{m}{i}$; see [6] for a proof for general W.

In addition to length and dimension, the third important parameter of a code C is its distance $\operatorname{dist}(C)$, which equals the minimum Hamming distance between two distinct codewords. For a linear code, one has $\operatorname{dist}(C) = \min_{x \in C \setminus \{0\}} \operatorname{wt}(x)$, where wt denotes the Hamming weight. The classical Reed–Muller codes are well known to have distance $\operatorname{dist}(RM(r, m)) = 2^{m-r}$ [10, Thm.13.3]. For a general Coxeter code $\mathsf{C}_W(r)$, it is clear from (1) that $\operatorname{dist}(\mathsf{C}_W(r))$ is at most the size of the smallest standard parabolic subgroup of rank $m-r$. Coble and Barg conjectured that this upper bound is in fact the exact distance for general Coxeter codes. In this paper, we prove this conjecture:

Theorem 1.1. *Let (W,S) be a finite Coxeter system of rank m and let $d_r := \min_{I\subseteq S, |I|=m-r} |W_I|$ be the order of the smallest parabolic subgroup of rank $m-r$. Then*

$$\mathrm{dist}(\mathsf{C}_W(r)) = d_r.$$

Our proof of Theorem 1.1 proceeds by reduction to certain projections of the code $\mathsf{C}_W(r)$ which we call *shadow codes*, and which we explore on their own merit, finding their bases and parameters. The core part of the proof is a lower bound on the distance of a shadow code, which is then taken back to the main code by peeling off fixed-rank layers starting from the top level. While our arguments are phrased in combinatorial terms, the key ideas of the proof can be adapted to produce a decoding algorithm for Coxeter codes that generalizes Reed's majority-logic decoding algorithm for Reed–Muller codes [12]. As one of our results, we uncover this connection in Sec. 5. Our decoding algorithm presented in Sec. 5.2 also yields another proof of Theorem 1.1.

2. Preliminaries

All codes that we mention are binary linear codes, all group actions are left actions, and all modules are left modules. For the rest of the paper, let (W,S) be a finite Coxeter system with rank $|S|=m$. Let ℓ and $\leq$ be the length function and Bruhat order on W, respectively. We recall that a *right descent* of an element $w\in W$ is an element $s\in S$ such that $ws<w$ (equivalently, such that $\ell(ws)<\ell(w)$), and we write $D_R(w)$ for the set of all right descents of w. For every $K\subseteq S$, we denote the set $S\setminus K$ by K^c and the standard parabolic subgroup $\langle K\rangle$ of W by W_K, we define

$$W^K = \{w\in W : D_R(w)\cap K=\varnothing\},$$

and we set

$$\left\langle {W \atop K} \right\rangle = \{w\in W : D_R(w)=K\}.$$

The numbers $|\left\langle {W \atop K} \right\rangle|$ refine the *Eulerian numbers* $\left\langle {W \atop i} \right\rangle$, defined as

$$\left\langle {W \atop i} \right\rangle = |\{w\in W : |D_R(w)|=i\}|,$$

in that $\left\langle {W \atop i} \right\rangle = \sum_{K\subseteq S, |K|=i} |\left\langle {W \atop K} \right\rangle|$.

Let

$$w\star s := \begin{cases} ws, & \text{if } ws>w,\\ w, & \text{if } ws<w \end{cases}$$

for any $w\in W$ and $s\in S$. For any word $\boldsymbol{s}=s_1\cdots s_m$, the *Demazure product* [7] of $\boldsymbol{s}$ is the recursively defined element

$$\delta(\boldsymbol{s}) = (((e\star s_1)\star s_2)\cdots)\star s_m \in W.$$

Note that if $w\in W$ is the element expressed by $\boldsymbol{s}$, then $\delta(\boldsymbol{s})=w$ if and only if $\boldsymbol{s}$ is a reduced word of w.

We will frequently use the following standard facts in this paper.

(C1) [4, Sec.2.2] If $w,u\in W$ and $\boldsymbol{s}=s_1\cdots s_m$ is a reduced word of w, then $u\leq w$ if and only if some subword of $\boldsymbol{s}$ is a reduced word of u, where by a subword of $\boldsymbol{s}$ we mean a word of the form $s_{i_1}\cdots s_{i_k}$ for some $1\leq i_1<\cdots<i_k\leq m$.

(C2) [8, Sec.2.3] (cf. [9, Lemma 3.4]) For any word $\boldsymbol{s} = s_1 \cdots s_m$, the Demazure product $\delta(\boldsymbol{s})$ is the unique Bruhat-maximal element of W that can be obtained as the product of a subword of $\boldsymbol{s}$. In particular, $\boldsymbol{s}$ contains a reduced word of $\delta(\boldsymbol{s})$ as a subword.

(C3) [4, Sec.2.3] A finite Coxeter system (W', S') has a unique maximal element, w_0, with respect to the Bruhat order. The element w_0 has order 2, and it is the unique element of W' such that $D_R(w_0) = S'$. We also have $D_R(w_0 w) = S' \setminus D_R(w)$ for all $w \in W'$.

(C4) [4, Sec.2.4] For any $I \subseteq S$, the pair (W_I, I) is also a Coxeter system, and for every $w \in W_I$ we have $\ell_I(w) = \ell(w)$, where ℓ_I stands for the length function associated with (W_I, I). For any $I, J \subseteq S$, we have $W_I \cap W_J = W_{I \cap J}$.

(C5) [4, Sec.2.4] For every $w \in W$ and $I \subseteq S$, there is a unique factorization $w = w^I w_I$, called the *(left) coset factorization of w with respect to I*, such that $w^I \in W^I$ and $w_I \in W_I$, and for this factorization we have $\ell(w) = \ell(w^I) + \ell(w_I)$.

For each $I \subseteq S$, we will denote the longest element of the parabolic subgroup $W_I \leq W$ by w_0^I. The following well-known facts follow readily from (C3)–(C5) and will be particularly useful in Sec. 3.

(C6) For any $I \subseteq S$ and any $w = w^I \cdot w_I \in W$, the element w^I is the unique minimal-length representative of the left coset wW_I, and the element $w^I w_0^I$ is the unique maximal-length coset representative of wW_I. The set of all minimal-length representatives of the left cosets of W_I, $\mathrm{MinRep}(I)$, coincides with W^I; the set of all maximal-length representatives of the left cosets of W_I, $\mathrm{MaxRep}(I)$, is given by

$$\mathrm{MaxRep}(I) = \{w \in W : w_I = w_0^I\} = \{w \in W : D_R(w_I) = I\}. \tag{3}$$

Furthermore, we have $D_R(w_I) = D_R(w) \cap I$ for any $w \in W$, so we also have

$$\mathrm{MaxRep}(I) = \{w \in W : I \subseteq D_R(w)\}. \tag{4}$$

Let $R = \mathbb{F}_2[W]$ be the group algebra of W over $\mathbb{F}_2$. Every element of R has the form $t_X = \sum_{w \in X} w$ for some $X \subseteq W$, in which case we will call X the *support* of t_X and identify t_X with the indicator function $\mathbb{1}_X$ on W. We write

$$b_I := t_{W_I} = \sum_{w \in W_I} w \in R$$

for each $I \subseteq S$, with $W_\varnothing = \{1_W\}$. It follows from (1) that we can view Coxeter codes as sums of suitable cyclic R-submodules of the form $Rb_I, I \subseteq S$. More precisely, for each $r \in \{-1, 0, \cdots, m\}$, we have

$$\mathsf{C}_W(r) = \sum_{I \subseteq S, |I| = m - r} R\, b_I.$$

Elements of the form wb_I will play an important role in this paper.

Lemma 2.1.

(a) *We have $wb_I = w'b_I$ if and only if $wW_I = w'W_I$.*

(b) *If $I \cap J \neq \varnothing$, then $b_I b_J = 0$ in $\mathbb{F}_2[W]$.*

Proof. Part (a) holds because the support of xb_I equals the coset xW_I for all $x \in W$. Part (b) follows from (C4) as follows. We have

$$b_I b_J = \sum_{u \in W_I} u \sum_{v \in W_J} v = \sum_{x \in W_I W_J} a_x x,$$

where a_x is the number of pairs (u, v) where $u \in W_I, v \in W_J$, and $uv = x$ for every $x \in W_I W_J$. It is a basic fact from group theory that this number is precisely the order of the group $W_I \cap W_J$.

We have $W_I \cap W_J = W_{I\cap J}$ by (C4), which has even order if $I \cap J \neq \varnothing$, so $a_x = 0$ for all $x \in W$ and $b_I b_J = 0$ whenever $I \cap J \neq \varnothing$. □

We recall from [6, Theorem 3.6, Theorem 4.1] that the set

$$\mathcal{B}_{m-r} := \{wb_J : J = S \setminus D_R(w) \text{ and } |J| \geq m-r\}$$

forms a basis of $\mathsf{C}_W(r)$, which also implies the expression for $\dim \mathsf{C}_W(r)$ in (2).

We will be using the following related but different basis of $\mathsf{C}_W(r)$ in this paper.

Proposition 2.2. *For every $r \in \{0, \ldots, m\}$, the set*

$$\mathcal{C}_{m-r} := \{wb_J : J = D_R(w), |J| \geq m-r\}$$

is a basis of $\mathsf{C}_W(r)$.

Proof. This fact has been mentioned without proof in [6, Sec.3.1], so we provide a short proof here. Consider the action of the longest element $w_0 \in W$ on $\mathsf{C}_W(r)$. Recall that $w_0^2 = 1_W$ and $D_R(w_0 w) = S \setminus D_R(w)$ for all $w \in W$ by (C3), so this action is an involutive linear map on $\mathsf{C}_W(r)$ that interchanges $\mathcal{B}_{m-r}$ and $\mathcal{C}_{m-r}$. Since $\mathcal{B}_{m-r}$ is a basis, it follows that so is $\mathcal{C}_{m-r}$. □

Remark 2.3. The fact that $D_R(w_0 w) = S \setminus D_R(w)$ for all $w \in W$ also implies that left multiplication by w_0 on W interchanges the sets $\left\langle {W \atop J} \right\rangle$ and $\left\langle {W \atop J^c} \right\rangle$ for any J, which implies that

$$\left\langle {W \atop i} \right\rangle = \left\langle {W \atop m-i} \right\rangle \tag{5}$$

for any $0 \leq i \leq m$. Eq. (5) is known as the *Dehn–Sommerville relation.*

3. Shadow codes

For $K \subseteq S$, let

$$M_K = \mathbb{F}_2[W/W_K].$$

Define the *K-shadow projection* to be the $\mathbb{F}_2$-linear map given by

$$\pi_K : R \to M_K, \quad w \mapsto wW_K,$$

and define the *K-lift* to be the $\mathbb{F}_2$-linear map given by

$$\iota_K : M_K \to R, \quad wW_K \mapsto wb_K.$$

Note that ι_K is well defined by Lemma 2.1(a). Note also that M_K has an R-module structure induced by the natural action of W on the left cosets of W_K, and that the shadow projection π_{K^c} is W-equivariant and is thus an R-module homomorphism.

Definition 3.1. For every $I \subseteq S$, we define the *shadow code of type I* to be the image

$$D_I = \pi_{I^c}(Rb_I),$$

viewed as a linear code in the vector space M_{I^c}, and we set

$$\mathcal{B}_I := \{\pi_{I^c}(wb_I) : D_R(w) = I\}.$$

For any $r \in \{-1, 0, \ldots, m\}$, denote

$$\mathcal{I}_{m-r} := \{I \subseteq S : |I| = m-r\}.$$

Further, let ϕ_r be the map

$$\phi_r : \mathsf{C}_W(r) \to \bigoplus_{I \in \mathcal{I}_{m-r}} D_I, \quad c \mapsto (\pi_{I^c}(c))_I\,. \tag{6}$$

The main goal of this section is to prove that for every $0 \leq r \leq m$, the natural embedding $\mathsf{C}_W(r-1) \hookrightarrow \mathsf{C}_W(r)$ followed by ϕ_r forms a short exact sequence. This is the content of Theorem 3.5. We will also show that $\mathcal{B}_I$ is a basis of the code D_I for all $I \subseteq S$.

Proposition 3.2. *Let $K \subseteq S$ and $x \in R$. Let $r = |K|$.*

(a) *If $x = \sum_{w \in W} a_w w \in R$, then*
$$\pi_K(x) = \sum_{\Omega \in W/W_K} \Big(\sum_{w \in \Omega} a_w \Big) \Omega.$$
(b) *The K-shadow projection weakly decreases weight:* $\mathrm{wt}(\pi_K(x)) \leq \mathrm{wt}(x)$.
(c) *We have $\iota_K \pi_K(x) = x b_K$, and $\pi_K(x) = 0$ if and only if $x b_K = 0$.*
(d) *For any $w \in W$ and any $J \subseteq S$ such that $J \cap K \neq \varnothing$, we have $\pi_K(w b_J) = 0$.*
(e) *We have $\pi_K(\mathsf{C}_W(r-1)) = 0$.*

Proof. If $x = \sum_{w \in W} a_w w$, then we have $\pi_K(x) = \sum_{w \in W} a_w w W_K$, so each coset $\Omega = u W_K$ of W_K appears with coefficient
$$\sum_{w \in W : w W_K = u W_K} a_w = \sum_{w \in \Omega} a_w.$$
Part (a) follows. It also follows that every coset in the support of $\pi_K(x)$ arises from at least one element in the support of x, so (b) holds as well.

We have $\iota_K \pi_K(w) = w b_K$ for any $w \in W$ by the definition of ι_K and π_K, so it follows from linearity that $\iota_K \pi_K(x) = x b_K$ for any $x \in R$.

Since distinct left cosets of W_K have disjoint support, the map ι_K is injective, so we have $\pi_K(x) = 0$ if and only if $\iota_K \pi_K(x) = 0$, which occurs if and only if $x b_K = 0$ by the preceding statement. This completes the proof of (c).

If $J \cap K \neq \varnothing$, then $(w b_J) b_K = w(b_J b_K) = 0$ by Lemma 2.1(b), so we have $\pi_K(w b_J) = 0$ by (c). This proves (d).

By Proposition 2.2, the set $\mathcal{C}_{m-(r-1)} = \{ w b_J : J = D_R(w), |J| \geq m - r + 1 \}$ is a basis of $\mathsf{C}_W(r-1)$. For every set $J \subseteq S$ with $|J| \geq m - r + 1$, we have $|K| + |J| = m + 1 > |S|$ and thus $K \cap J \neq \varnothing$, so every element of $\mathcal{C}_{m-(r-1)}$ vanishes under π_K by (d). It follows that $\pi_K(\mathsf{C}_W(r-1)) = 0$, which proves (e). □

Corollary 3.3. *The map ϕ_r is surjective.*

Proof. Let $z = (z_I)_I \in \bigoplus_{I \in \mathcal{I}_{m-r}} D_I$. By the definition of D_I, there exists $c_I \in R b_I$ such that $z_I = \pi_{I^c}(c_I)$ for each $I \in \mathcal{I}_{m-r}$. Set $c = \sum_{J \in \mathcal{I}_{m-r}} c_J$. For any two distinct sets $I, J \in \mathcal{I}_{m-r}$, we have $I^c \cap J \neq \varnothing$, so Proposition 3.2(d) implies $\pi_{I^c}(c_J) = 0$. This further implies that the I-component of $\phi_r(c)$ is
$$\phi_I(c) := \pi_{I^c}\Big(\sum_{J \in \mathcal{I}_{m-r}} c_J \Big) = \pi_{I^c}(c_I) = z_I$$
for every $I \in \mathcal{I}_{m-r}$, so $\phi_r(c) = z$. It follows that ϕ_r is surjective, as desired. □

The next result proves the linear independence of the set $\mathcal{B}_I$. We will use it to help prove $\ker \phi_r = \mathsf{C}_W(r-1)$, which we will then use to help prove that $\mathcal{B}_I$ is in fact a basis of D_I.

Proposition 3.4. *For any $I \subseteq S$, the map*
$$f_I : \left\langle \begin{matrix} W \\ I \end{matrix} \right\rangle \to \mathcal{B}_I, \quad w \mapsto \pi_{I^c}(w b_I)$$
is a bijection. The elements of the set $\mathcal{B}_I$ are linearly independent over $\mathbb{F}_2$.

Proof. Let $w \in \left\langle {W \atop I} \right\rangle$, so that $D_R(w) = I$. Proposition 3.2(c) implies that

$$\iota_{I^c}(f_I(w)) = \iota_{I^c}\pi_{I^c}(wb_I) = wb_I b_{I^c} = \sum_{u \in wW_I, y \in W_{I^c}} uy \in R.$$

Set $z = w_0^{I^c}$, the unique longest element in the parabolic subgroup W_{I^c}. Since $D_R(w) = I$, it follows from (C5) that the coset factorization of the element wz with respect to I^c is simply $wz = w \cdot z$, with $\ell(wz) = \ell(w) + \ell(z)$, and it follows from (C6) that w is the unique maximal-length element in the coset wW_I. Thus, for any pair of elements $u \in wW_I$ and $y \in W_{I^c}$, we have

$$\ell(uy) \leq \ell(u) + \ell(y) \leq \ell(w) + \ell(z) = \ell(wz),$$

where $\ell(uy) = \ell(wz)$ if and only if $u = w$ and $y = z$. This implies that the element $w' := wz$ is the unique longest element in the support of $\iota_{I^c}(f_I(w))$. Thus, we may recover w from $f_I(w)$ by taking the I^c-lift, finding the unique longest element w' in the support of the I^c-lift, and then computing w as $w = w'z^{-1}$. This implies f_I is injective.

We also have $\operatorname{im} f_I = \mathcal{B}_I$ by the definition of f_I and $\mathcal{B}_I$, so f_I is a bijection.

It remains to show that $\mathcal{B}_I = \operatorname{im} f_I$ is linearly independent. Suppose $\sum_{j=1}^k a_j f_I(w_j) = 0$ for some scalars $a_1, \ldots, a_k \in \mathbb{F}_2$ and distinct elements $w_1, ..., w_k \in \left\langle {W \atop I} \right\rangle$. By the last paragraph, if w_i is any element in $w_1, \ldots, w_k$ with maximal length, then in the I^c-lift

$$\iota_{I^c}\Big(\sum_{j=1}^k a_j f_I(w_j)\Big) = \sum_{j=1}^k a_j \left(\iota_{I^c} f_I(w_j)\right) \in R$$

the element $w_i z$ is a maximal-length element that appears with coefficient a_i, so $a_i = 0$. It follows by induction on k that $a_j = 0$ for all $1 \leq j \leq k$, so $\mathcal{B}_I$ is linearly independent, as desired. □

It is important to note that Theorem 3.5 below allows us to prove the main distance result using induction. Indeed, the fact that there is a short exact sequence as in the theorem means that a codeword $c \in C_W(r)$ either lies in $C_W(r-1)$ or projects non-trivially onto the direct sum, where we will be able to have precise control over the distances of the shadow codes D_I (Proposition 4.5). We will use the distances of these shadow codes and the fact that shadow projections do not increase weight to prove Theorem 1.1.

Theorem 3.5. *For every $r \in \{0, \ldots, m\}$, we have a short exact sequence of R-modules given by*

$$0 \longrightarrow \mathsf{C}_W(r-1) \xhookrightarrow{\psi_{r-1}} \mathsf{C}_W(r) \xrightarrow{\phi_r} \bigoplus_{I \in \mathcal{I}_{m-r}} D_I \longrightarrow 0, \tag{7}$$

where ψ_{r-1} is the natural embedding of $\mathsf{C}_W(r-1)$ into $\mathsf{C}_W(r)$.

Proof. The map ψ_{r-1} is an injective R-module homomorphism because it is a natural embedding. The map ϕ_r is an R-module homomorphism because we have noted that ϕ_I is an R-module homomorphism for every $I \subseteq S$, and ϕ_r is surjective by Corollary 3.3. It remains to show that $\operatorname{im} \psi_{r-1} = \ker \phi_r$. In other words, it suffices to show that $\mathsf{C}_W(r-1) = \ker \phi_r$. Proposition 3.2(d) implies that $\pi_{I^c}(\mathsf{C}_W(r-1)) = 0$ for all $I \in \mathcal{I}_{m-r}$, so we have $\mathsf{C}_W(r-1) \subseteq \ker \phi_r$ and it further suffices to show that $\ker \phi_r \subseteq \mathsf{C}_W(r-1)$.

Let $c \in \ker \phi_r \subseteq \mathsf{C}_W(r)$. Expand c into the basis $\mathcal{C}_{m-r}$ of $\mathsf{C}_W(r)$ as

$$c = \sum_{w : |D_R(w)| \geq m-r} a_w e_w,$$

where $e_w = wb_{D_R(w)}$ for every w. If $|D_R(w)| > m-r$, then e_w lies in the basis $\mathcal{C}_{m-(r-1)}$ of $\mathsf{C}_W(r-1)$, so $\phi_r(e_w) = 0$ since $\mathsf{C}_W(r-1) \subseteq \ker \phi_r$. It follows that

$$0 = \phi_r(c) = \sum_{w:|D_R(w)=m-r|} \phi_r(a_w e_w).$$

Now fix a set $I \subseteq S$ with $|I| = m-r$. Taking the I-component of the above sum yields

$$0 = \sum_{w:|D_R(w)|=m-r} a_w \pi_{I^c}(e_w) = \sum_{J\in\mathcal{I}_{m-r}} \sum_{w\in\left\langle {W \atop J} \right\rangle} a_w \pi_{I^c}(e_w).$$

For any $J \in \mathcal{I}_{m-r} \setminus \{I\}$, we have $I^c \cap J \neq \varnothing$, and therefore $\pi_{I^c}(e_w) = 0$ for all $w \in \left\langle {W \atop J} \right\rangle$ by Proposition 3.2(d). It then follows that

$$\sum_{w:w\in\left\langle {W \atop I} \right\rangle} a_w \pi_{I^c}(e_w) = 0.$$

The set $\{\pi_{I^c} e_w : w \in \left\langle {W \atop I} \right\rangle\}$ is precisely the set $\mathcal{B}_I$, so Proposition 3.4 implies that $a_w = 0$ for all $w \in \left\langle {W \atop I} \right\rangle$. Since I is arbitrary, it follows that $a_w = 0$ for all $w \in W$ with $|D_R(w)| = m-r$, so c is in the span of the basis $\mathcal{C}_{m-(r-1)}$ of $\mathsf{C}_W(r-1)$. This proves $\ker \phi_r \subseteq \mathsf{C}_W(r-1)$, as desired. □

The next theorem is not needed to show our main result and is included to provide an additional insight into the properties of shadow codes.

Theorem 3.6. *For any $I \subseteq S$, the set $\mathcal{B}_I = \{\pi_{I^c}(wb_I) : D_R(w) = I\}$ is a basis of the shadow code D_I, and we have*

$$\dim D_I = \left| \left\langle {W \atop I} \right\rangle \right|.$$

Proof. Let $I \subseteq S$ and suppose $|I| = m-r$ for some $0 \leq r \leq m$. Proposition 3.4 implies that $|\mathcal{B}_I| = \left| \left\langle {W \atop I} \right\rangle \right|$, so it suffices to prove that $\mathcal{B}_I$ is a basis of D_I.

For all $J \in \mathcal{I}_{m-r}$, the set $\mathcal{B}_J$ is linearly independent by Proposition 3.4, so we have $\dim D_J \geq |B_J|$, where equality holds if and only if B_J is a basis for D_J. Since $|B_J| = \left\langle {W \atop J} \right\rangle$ by Proposition 3.4, it follows that

$$\dim \bigoplus_{J\in\mathcal{I}_{m-r}} D_J = \sum_{J\in\mathcal{I}_{m-r}} \dim D_J \geq \sum_{J\in\mathcal{I}_{m-r}} |\mathcal{B}_J| = \sum_{J\in\mathcal{I}_{m-r}} \left\langle {W \atop J} \right\rangle = \left\langle {W \atop m-r} \right\rangle,$$

with $\dim \bigoplus_{J\in\mathcal{I}_{m-r}} D_J = \left\langle {W \atop m-r} \right\rangle$ if and only if $\mathcal{B}_J$ is a basis of D_J for all $J \in \mathcal{I}_{m-r}$. Thus, to prove the theorem it further suffices to show that $\dim \bigoplus_{J\in\mathcal{I}_{m-r}} D_J = \left\langle {W \atop m-r} \right\rangle$. This follows from Theorem 3.5 as follows: since the map $\phi_r : \mathsf{C}_W(r) \to \bigoplus_{I\in\mathcal{I}_{m-r}} D_I$ is surjective and has $\mathsf{C}_W(r-1)$ as its kernel by Theorem 3.5, we have

$$\begin{aligned}\dim \bigoplus_{J\in\mathcal{I}_{m-r}} D_J &= \dim \mathsf{C}_W(r) - \dim \mathsf{C}_W(r-1) \\ &= \sum_{i=0}^{r} \left\langle {W \atop i} \right\rangle - \sum_{i=0}^{r-1} \left\langle {W \atop i} \right\rangle \\ &= \left\langle {W \atop r} \right\rangle = \left\langle {W \atop m-r} \right\rangle,\end{aligned}$$

where the second and fourth equalities hold by Eqns. (2) and (5), respectively. □

4. Minimum distance of Coxeter codes

In this section, we prove Theorem 1.1. We will first show that $\mathrm{dist}(D_I) = |W_I|$ for any $I \subseteq S$ (Proposition 4.5), which we will then combine with Theorem 3.5 to deduce Theorem 1.1.

Definition 4.1.

(1) For any $I \subseteq S$ and $s \in I$, we define the *s-coarsening of M_{I^c}* to be the $\mathbb{F}_2$-linear map

$$\rho_{s,I} : M_{I^c} \to M_{I^c \cup \{s\}}, \quad wW_{I^c} \mapsto wW_{I^c \cup \{s\}},$$

and we write $\rho_{s,I}$ as ρ_s if I is clear from context.

(2) For each $x \in W$, we define the *I-apartment indexed by x* to be the set

$$\Sigma_x := \{\, xu\, W_{I^c} : u \in W_I \,\} \subseteq W/W_{I^c}.$$

We call each element in Σ_x an *I-chamber.*

Note that $\rho_{s,I}$ is well defined because $W_{I^c} \leq W_{I^c \cup \{s\}}$. The map sending each $u \in W_I$ to the coset xuW_{I^c} is injective, because if $xuW_{I^c} = xu'W_{I^c}$ for $u, u' \in W_I$ then we have $u^{-1}u' \in W_{I^c} \cap W_I = W_{I \cap I^c} = \{1_W\}$, so each I-apartment Σ_x consists of $|W_I|$ distinct chambers.

Lemma 4.2. *If $s \in I \in \mathcal{I}_{m-r}$ for some $0 \leq r \leq m$, then we have $\rho_s(D_I) = 0$.*

Proof. It suffices to show that $\rho_s(\pi_{I^c}(wb_I)) = 0$ for any $w \in W$. We have

$$\rho_s\big(\pi_{I^c}(wb_I)\big) = \sum_{u \in W_I} wu\, W_{I^c \cup \{s\}}. \tag{8}$$

For any $u_1, u_2 \in W_I$, we have $wu_1W_{I^c \cup \{s\}} = wu_2W_{I^c \cup \{s\}}$ if and only if

$$u_1^{-1}u_2 \in W_I \cap W_{I^c \cup \{s\}} = W_{I \cap (I^c \cup \{s\})} = W_{\{s\}},$$

where the first set equality holds by (C4). It follows that the fibers of the map $W_I \to W/W_{I^c \cup \{s\}}$, $u \mapsto wu\, W_{I^c \cup \{s\}}$ are simply the cosets of $W_{\{s\}}$ in W_I. All of these cosets have size $\left|W_{\{s\}}\right| = |\{1_W, s\}| = 2$, so Eq. (8) implies that $\rho_s(\pi_{I^c}(wb_I)) = 0$, as desired. $\square$

Lemma 4.3 (Parabolic Bruhat projection)**.** *For each $w \in W$ the set $\{u \in W_I : u \leq w\}$ has a unique maximum element, denoted $\beta_I(w) \in W_I$, with respect to the Bruhat order. Moreover, for every $s \in I$, every $y \in W^{I^c \cup \{s\}}$, and every $q \in W_{I^c \cup \{s\}}$, we have*

$$\beta_I(yq) \in \beta_I(y)\, W_{\{s\}} = \{\beta_I(y), \beta_I(y)s\}.$$

Proof. Fix a reduced word $\boldsymbol{s} = s_1 \cdots s_m$ of w, and let $\boldsymbol{t}$ be the subword of $\boldsymbol{s}$ obtained by removing all letters s_i not in I. Put $b := \delta(t) \in W_I$. The word $\boldsymbol{t}$ contains a reduced word of b as a subword by (C2), and hence so does $\boldsymbol{s}$, which implies that $b \leq w$ by (C1). Conversely, if $u \in W_I$ and $u \leq w$, then (C1) implies that some subword of $s_1 \cdots s_m$ is a reduced word for u. Since $u \in W_I$, this subword uses only letters from I, so it is a subword of t and $u \leq \delta(t) = b$ by (C2). It follows that b is the unique maximum element of the set $\{u \in W_I : u \leq w\}$ (and is independent of the choice of the reduced word $\boldsymbol{t}$); in other words, we have $\beta_I(w) = \delta(\boldsymbol{t})$.

For the second assertion, let $s \in I, y \in W^{I^c \cup \{s\}}$ and $q \in W_{I^c \cup \{s\}}$. By (C5), we have $\ell(yq) = \ell(y) + \ell(q)$, so concatenating a reduced word $\boldsymbol{s}$ of y with a reduced word $\boldsymbol{t}$ of q produces a reduced word for yq. Since $q \in W_{I^c \cup \{s\}}$, the only letter from I that may appear in $\boldsymbol{t}$ is s, so it follows from the last paragraph and the definition of $\star$ that

$$\beta_I(yq) = \delta(\boldsymbol{st}) = (((\delta(\boldsymbol{s}) \star s)\star) \cdots \star s) = (((\beta_I(y) \star s) \star s) \cdots \star s) \in \beta_I(y)W_{\{s\}}.$$

This completes the proof. $\square$

Lemma 4.4 (Rank-selected retraction)**.** *Fix $x \in W^{I^c}$ and let $C := xW_{I^c} \in \Sigma_x$. Consider the map $r_x : W/W_{I^c} \to \Sigma_x$ given by $\Omega \mapsto xr_0(x^{-1}\Omega)$, where $r_0(vW_{I^c}) = \beta_I(v)W_{I^c}$ for any minimum-length coset representative $v \in W^{I^c}$ (and $\beta_I(v)$ is as defined in Lemma 4.3). Then*

- (a) *r_x fixes the apartment Σ_x pointwise;*
- (b) *for each $s \in I$, r_x carries every fiber of ρ_s into a single fiber of ρ_s; consequently, there is a map $r^{(s)} : W/W_{I^c \cup \{s\}} \to W/W_{I^c \cup \{s\}}$ such that $\rho_s \circ r_x = r^{(s)} \circ \rho_s$;*
- (c) *$r_x^{-1}(C) = \{C\}$.*

Proof. We first treat the case $x = 1_W$, where $C = C_0 := W_{I^c}$, $\Sigma_x = \Sigma_0 := \{uW_{I^c} : u \in W_I\}$, and $r_x = r_0$. Let us prove that the mapping r_0 satisfies properties (a)–(c).

(a) Each chamber in Σ takes the form $\Omega = uW_{I^c} \in \Sigma_0$ for some $u \in W_I$. We have $D_R(u) \subseteq I$, so $u \in W^{I^c}$ and u is the minimal representative of Ω by (C6). Since $u \in W_I$, we also have $\beta_I(u) = u$ by Lemma 4.3, so $r_0(\Omega) = r_0(uW_{I^c}) = \beta_I(u)W_{I^c} = uW_{I^c} = \Omega$.

(b) Fix $s \in I$ and put $J := I^c \cup \{s\}$. If wW_{I^c} is a coset in a fiber $\rho_s^{-1}(yW_J)$, where $w \in W^{I^c}$ and $y \in W^J$ are the respective minimal representatives of wW_{I^c} and yW_J, then we have $w = yq$ for some $q \in W_J$ such that $\ell(w) = \ell(y) + \ell(q)$ by (C5), and (C4) then implies that $q \in W^{I^c}$ (because the condition $\ell(w) = \ell(y) + \ell(q)$ implies $D_R(q) \cap I^c \subseteq D_R(w) \cap I^c = \varnothing$). Lemma 4.3 now implies that

$$r_0(wW_{I^c}) = \beta_I(w)\, W_{I^c} = \beta_I(yq)\, W_{I^c} \in \{\beta_I(y)\, W_{I^c}, \beta_I(y)s\, W_{I^c}\} \subseteq \rho_s^{-1}(\beta_I(y)W_J),$$

so r_0 maps every coset in the fiber $\rho_s^{-1}(yW_J)$ to the fiber $\rho_s^{-1}(\beta_I(y)W_J)$. Consequently, we have $\rho_s \circ r_0 = r_0^{(s)} \circ \rho_s$ for the map $r_0^{(s)} : W/W_J \to W/W_J, yW_J \mapsto \beta_I(y)W_J$.

(c) Suppose $r_0(vW_{I^c}) = C_0$ with $v \in W^{I^c}$. Then $\beta_I(v) \in W_{I^c} \cap W_I = \{1_W\}$, so $\beta_I(v) = 1_W$. If $v \neq 1_W$, fix a reduced word $\boldsymbol{s}$ for v. If all letters in $\boldsymbol{s}$ are in I^c, then $v \in W_{I^c} \cap W^{I^c} = \{1_W\}$, a contradiction; if some letter s in $\boldsymbol{s}$ is from I, then (C2) implies that $s \leq \beta_I(v) = e$, which is again a contradiction. Therefore $v = 1_W$ and $r_0^{-1}(C_0) = \{C_0\}$.

We have proved that $r_x = r_0$ satisfies conditions (a)–(c) when $x = e$. Let us prove the case of a general x. We have $x^{-1}\Sigma_x = \Sigma_0$ and $x^{-1}C = C_0$, and ρ_s is W-equivariant, so (a)–(c) transfer verbatim, with $r^{(s)}(Q) := x\, r_0^{(s)}(x^{-1}Q)$ for every coset Q of $W_{I^c \cup \{s\}}$. □

We will refer to each map of the form r_x as a *rank-selected retraction.* These retraction maps form the core component of the following proof, as well as of the decoder of Coxeter codes in Sec. 5; see the example in Sec. 5.3 for an illustration.

Proposition 4.5 (Shadow distance)**.** *Let $I \subseteq S$. The distance of the shadow code equals*

$$\mathrm{dist}(D_I) = |W_I|.$$

Proof. If $I = \varnothing$, then $I^c = S$, and $D_I = D_\varnothing = \mathbb{F}_2[W/W_S] \cong \mathbb{F}_2$ has distance $1 = |W_I|$ as desired, so assume $I \neq \varnothing$.

The element $\pi_{I^c}(b_I) \in D_I$ has weight at most $\mathrm{wt}(b_I) = |W_I|$ by Proposition 3.2(b), so we have $\mathrm{dist}(D_I) \leq |W_I|$ and it remains to prove the reverse inequality. Let $z \in D_I \backslash \{0\}$. Choose a coset $C = xW_{I^c} \in \mathrm{supp}(z)$ with minimal representative $x \in W^{I^c}$. This is a chamber in the I-apartment $\Sigma := \Sigma_x$. Now let $r_x : W/W_{I^c} \to \Sigma_x$ be as in Lemma 4.4. Overloading the notation, let us extend r_x linearly to a map $r_x : M_{I^c} \to \mathbb{F}_2[\Sigma_x] \subseteq M_{I^c}$, and set $z_\Sigma := r_x(z)$. Note that $z_\Sigma \neq 0$: by property (c) of Lemma 4.4, C is the only chamber in Σ_x mapped to C by r_x, so the coefficient of C in z_Σ equals its coefficient in z, namely, 1.

For any $s \in I$, we have $\rho_s(z) = 0$ by Lemma 4.2, so it follows from property (b) of Lemma 4.4 that

$$\rho_s(z_\Sigma) = \rho_s\, r_x(z) = r^{(s)}\, \rho_s(z) = 0;$$

that is, z_Σ vanishes under every s-coarsening map.

Now write $z_\Sigma = \sum_{u\in W_I} a_u\, xu\, W_{I^c}$ with $a_u \in \mathbb{F}_2$. Fix $s \in I$. Two chambers xuW_{I^c}, xvW_{I^c} of Σ_x lie in the same ρ_s-fiber if and only if $xuW_{I^c\cup\{s\}} = xvW_{I^c\cup\{s\}}$, i.e., if and only if

$$u^{-1}v \in W_I \cap W_{I^c\cup\{s\}} = W_{\{s\}} = \{e, s\}.$$

This implies that the ρ_s-fibers in Σ_x are exactly the pairs $\{xuW_{I^c}, xus\,W_{I^c}\}$ where $u \in W_I$. The fact that $\rho_s(z_\Sigma) = 0$ now forces $a_u + a_{us} = 0$, i.e.,

$$a_u = a_{us}, \quad \text{for all } u \in W_I,\ s \in I.$$

These relations say that $u \mapsto a_u$ is constant along the edges of the Cayley graph of W_I with generating set I. Since this graph is connected, all the coefficients a_u are equal; since $z_\Sigma \neq 0$, they all equal 1. It follows that $z_\Sigma = \sum_{u\in W_I} xu\, W_{I^c}$ and $\mathrm{wt}(z_\Sigma) = |W_I|$.

Finally, the linear map r_x sends each basis element of M_{I^c} to a basis element of $\mathbb{F}_2[\Sigma_x]$, so it can only merge or cancel coordinates and never increases weight, and therefore $\mathrm{wt}(z) \geq \mathrm{wt}(z_\Sigma) = |W_I|$. As our choice of $z \in D_I\backslash\{0\}$ was arbitrary, it follows that $\mathrm{dist}(D_I) \geq |W_I|$, as desired. □

Proof of Theorem 1.1. We prove this by induction on r. For the base case, the code $\mathsf{C}_W(0) = \{0^{|W|}, 1^{|W|}\}$ has distance $|W| = d_0$. Now let us assume that the statement is true for $\mathsf{C}_W(r-1)$ for some $r \geq 1$. Let $c \in \mathsf{C}_W(r)\backslash\{0\}$. If $\phi_r(c) = 0$, then by Theorem 3.5 we conclude that $c \in \mathsf{C}_W(r-1)$, and thus $\mathrm{wt}(c) \geq d_{r-1}$ by the induction hypothesis. Next, notice that $d_{r-1} \geq d_r$. Indeed, let $I \subseteq S, |I| = m-r+1$ be such that $d_{r-1} = |W_I|$. Take $J \subset I$ with $|J| = m-r$ and observe that $d_{r-1} = |W_I| \geq |W_J| \geq d_r$. In conclusion, $\mathrm{wt}(c) \geq d_r$.

Now suppose that $\phi_r(c) \neq 0$, then for some I of size $m-r$, we have $\pi_{I^c}(c) \in D_I\backslash\{0\}$, and so $\mathrm{wt}(\pi_{I^c}(c)) \geq |W_I|$ by Proposition 4.5. Now Proposition 3.2(b) implies that $\mathrm{wt}(c) \geq \mathrm{wt}(\pi_{I^c}(c)) \geq d_r$, completing the induction. Finally, note that if d_r is attained for W_I with some I of size $m-r$, then the code $\mathsf{C}_W(r)$ contains the indicator vector of b_I, proving the equality in the statement. □

Remark 4.6. We note that in the case where $r \geq \lfloor \frac{m}{2} \rfloor$, the conclusion of Theorem 1.1 is already proved in [6, Cor.4.7], where the proof uses the well-known classification of finite Coxeter systems and the fact that all such systems have bipartite Coxeter graphs. Our approach via the reduction to shadow codes is somewhat more involved by comparison, but it allows us to treat all possible values of r at once, without relying on the classification.

5. Majority-logic decoding of Coxeter codes

Shortly after the discovery of RM codes by Muller [11], Reed introduced an algorithm for their decoding that corrects any combination of errors up to half the code's minimum distance [12], which we now generalize to arbitrary Coxeter codes. To build intuition, we begin with a brief overview of Reed's decoder. The encoding map of $RM(r, m)$ sends an *information vector* $\mu \in \mathbb{Z}_2^{\binom{m}{\leq r}}$ to a codeword $c \in \mathbb{Z}_2^{2^m}$, where $\binom{m}{\leq r} := \sum_{i=0}^r \binom{m}{i}$ is the code's dimension. Specifically, consider the set $V_r = \{v \in \mathbb{Z}_2^m : 0 \leq \mathrm{wt}(v) \leq r\}$ with $|V_r| = \binom{m}{\leq r}$, and write $\mu = (\mu_v)_{v\in V_r}$. Define a Boolean polynomial $f(x_1, \ldots, x_m) = \sum_{v\in V_r} \mu_v x_1^{v_1} \ldots x_m^{v_m}$; then μ is encoded into the code vector $c = (c_w, w \in \mathbb{Z}^{2^m})$ such that

$$c_w = f(w_1, \ldots, w_m) \qquad \text{for all } w = (w_1, \ldots, w_m).$$

Reed's algorithm recursively recovers the coefficients μ_v for v of decreasing Hamming weight and is a combination of the following observations:

(1) The code $RM(r, m)$ is spanned by indicators of all affine subspaces $\langle e_{i_1}, \ldots, e_{i_k}\rangle$ of $\mathbb{Z}_2^m$ of dimension $k \geq (m-r)$;

(2) Given an $(m-r)$-dimensional (linear) subspace $L \subset \mathbb{Z}_2^m$ spanned by $e_1, \dots, e_{m-r}$ (say) the subspace spanned by $e_{m-r+1}, \dots, e_m$ and its cosets each intersect L on a single symbol. These intersections form parity checks for the coefficients μ_v with $\mathrm{wt}(v) = r$. If the count of errors is not too high, the majority vote recovers all μ_v correctly. Subtracting the corresponding part of $f(x)$, we reduce the decoding problem to the code $RM(r-1, m)$, whose distance is twice that of $RM(r, m)$, and repeat the majority vote for the coefficients $\mu_v, \mathrm{wt}(v) = r - 1$. At the last step of the recursion, $r = 0$, the remaining part of $f(x)$ is just the constant term μ_0, and the corresponding code is the repetition code $RM(0, m)$.

See [10, Sec.13.6] for a detailed presentation.

In this section, we extend this idea to Coxeter codes. While this requires some adjustments, the general approach still relies on majority votes, and it specializes to the original RM decoder sketched above if $W = \mathbb{Z}_2^m$.

Fix $r \in \{0, 1, \dots, m\}$. By Proposition 2.2, the code $\mathsf{C}_W(r)$ has the descent basis

$$\mathcal{C}_{m-r} = \{\, e_w : |D_R(w)| \geq m - r\}, \qquad e_w := w\, b_{D_R(w)} = \mathbb{1}_{wW_{D_R(w)}}.$$

Thus a codeword $c \in \mathsf{C}_W(r)$ is the encoding of its *information symbols* $(\mu_w)_{|D_R(w)| \geq m-r}$, $\mu_w \in \mathbb{F}_2$ through

$$c = \sum_{w:\, |D_R(w)| \geq m-r} \mu_w\, e_w. \tag{9}$$

Recall that the shadow map ϕ_k defined in (6) isolates a single descent layer,

$$\pi_{I^c}(c) = \sum_{w:\, D_R(w) = I} \mu_w\, \pi_{I^c}(w b_I) \ \in \ D_I. \tag{10}$$

5.1. **Parity checks from apartments.** Let $y = c + \epsilon \in \mathbb{F}_2^{|W|}$, where $c \in \mathsf{C}_W(r)$ and ϵ is an error vector. We construct a set of equations (parity checks) that recover the coefficients μ_w by a majority vote. For $k \leq r$, fix $I \in \mathcal{I}_{m-k}$ and w with $D_R(w) = I$. Then $w \in W^{I^c}$ is the minimal-length representative of the chamber $C_w := wW_{I^c}$, and $\Sigma_w = \{wu\, W_{I^c} : u \in W_I\}$ is the apartment 'centered' at C_w. Let $r_w : W/W_{I^c} \to \Sigma_w$ be the rank-selected retraction of Lemma 4.4 centered at C_w, with $r_w(\Omega) = w\, r_0(w^{-1}\Omega)$ where $r_0(vW_{I^c}) = \beta_I(v)W_{I^c}$ for any minimal representative $v \in W^{I^c}$. Its fibers partition W/W_{I^c}, so pulling back along $W \to W/W_{I^c}$ partitions W into $|W_I|$ blocks indexed by $u \in W_I$:

$$T_w^{(u)} := \{\, g \in W :\ r_w(gW_{I^c}) = wu\, W_{I^c}\,\} = \{\, g \in W :\ \beta_I\big((w^{-1}g)^{I^c}\big) = u\,\}, \tag{11}$$

where $(\,\cdot\,)^{I^c}$ denotes the minimal-length representative modulo W_{I^c}; see (C5). The *u-th parity check at w* of y is

$$V_w^{(u)}(y) := \sum_{g \in T_w^{(u)}} y_g \ \in \ \mathbb{F}_2, \qquad u \in W_I.$$

The following lemma is formulated to fit the recursion of the decoding algorithm of Sec. 5.2 below; in particular, k refers to the order of the subcode $\mathsf{C}_W(k) \subset \mathsf{C}_W(r)$ that arises in the corresponding recursion step.

Lemma 5.1.
(a) *For $k \in \{0, 1, \dots, r\}$, let $I \in \mathcal{I}_{m-k}$, let w satisfy $D_R(w) = I$, and let $c' = \sum_{w'} \mu_{w'} e_{w'} \in \mathsf{C}_W(k)$ be a codeword with*

$$\mu_{w'} = 0 \quad \text{for every } w' \text{ with } D_R(w') = I \text{ and } w' > w. \tag{12}$$

Then $V_w^{(u)}(c') = \mu_w$ for every $u \in W_I$.
(b) *Let $\epsilon \in \mathbb{F}_2^{|W|}$ and let $y = c' + \epsilon$. If $\mathrm{wt}(\epsilon) < \frac{1}{2}|W_I|$, then $\mathrm{maj}_{u \in W_I} V_w^{(u)}(y) = \mu_w$.*

Proof. (a) Each block $T_w^{(u)}$ is a union of left W_{I^c}-cosets, so $V_w^{(u)}(y)$ equals the sum, over the fiber $r_w^{-1}(wuW_{I^c})$, of the coordinates of $\pi_{I^c}(y)$; that is, $V_w^{(u)}(y)$ is the coefficient of wuW_{I^c} in the vector $r_w\big(\pi_{I^c}(y)\big) \in \mathbb{F}_2[\Sigma_w]$.

We will first assume that $\epsilon = 0$ and so $y = c'$, and discuss the general ϵ later. By (10) we have $z := \pi_{I^c}(c') \in D_I$, so $\rho_s(z) = 0$ for all $s \in I$ by Lemma 4.2. The argument of Proposition 4.5 then shows that $r_w(z)$ has all its coefficients on Σ_w equal, with common value the coefficient of z at the center C_w (the center has the unique preimage $r_w^{-1}(C_w) = \{C_w\}$). Hence

$$V_w^{(u)}(c') = [\,\pi_{I^c}(c')\,]_{C_w} \quad \text{for all } u \in W_I.$$

Now $\pi_{I^c}(w'b_I) = \sum_{u' \in W_I} w'u'W_{I^c}$ is the indicator of the chamber set $\Sigma_{w'}$ with every coefficient equal to 1 since the terms in the sum are pairwise distinct basis vectors of M_{I^c}. Therefore, its coefficient at C_w is $N(w,w') := \mathbb{1}[\,C_w \in \Sigma_{w'}\,] \in \{0,1\}$, and by (10)

$$[\,\pi_{I^c}(c')\,]_{C_w} = \sum_{w' :\, D_R(w') = I} \mu_{w'}\, N(w,w'). \tag{13}$$

Suppose that $N(w,w') = 1$, i.e., $C_w \in \Sigma_{w'}$, or $wW_{I^c} \cap w'W_I \neq \varnothing$. Choose $a \in W_I$ with $w'a \in wW_{I^c}$. As $D_R(w') \supseteq I$, the element w' is the longest and hence the Bruhat-largest element of $w'W_I$ by (C6), so $w'a \le w'$; and $w = (w'a)^{I^c} \le w'a$ since a minimal coset representative lies below every element of its coset. Thus $N(w,w') = 1$ implies that $w \le w'$, and $N(w,w) = 1$ since $C_w \in \Sigma_w$, so the matrix N is triangular with 1's on the main diagonal. In the sum in (13) every term with $w' \neq w$ vanishes. Specifically, the terms with $w' < w$ vanish because $N(w,w') = 0$, and the terms with $w' > w$ vanish because $\mu_{w'} = 0$ by (12). Only the diagonal term $N(w,w)\mu_w$ remains, so $[\,\pi_{I^c}(c')\,]_{C_w} = \mu_w$, and therefore $V_w^{(u)}(c') = \mu_w$ for all u, proving Part (a).

(b) For $y = c' + \epsilon$ we have $V_w^{(u)}(y) = \mu_w + \sum_{g \in T_w^{(u)}} e_g$. As the blocks $T_w^{(u)}$ are pairwise disjoint, the number of u with $\sum_{g \in T_w^{(u)}} e_g \neq 0$ is at most $\mathrm{wt}(\epsilon)$; so if $\mathrm{wt}(\epsilon) < \frac{1}{2}|W_I|$, then fewer than half of the $|W_I|$ votes are flipped, and the majority returns μ_w. □

Remark 5.2. Assumption (12) is added to simplify the processing; without it, we would still be able to arrive at the same conclusions, but the assembled votes would form a triangular system of equations, requiring an extra step for the recovery of the individual coefficients.

5.2. **The decoder.**

Majority-logic decoder for $\mathsf{C}_W(r)$.

Input: a vector $y = c + \epsilon \in \mathbb{F}_2^{|W|}$

Output: symbols $(\mu_w)_{|D_R(w)| \ge m-r}$, cf. Eq. (9)

(1) For $k = r, r-1, \ldots, 0$:
   (a) For each $I \in \mathcal{I}_{m-k}$ and each w with $D_R(w) = I$, processed in order of *decreasing* length $\ell(w)$:
      (i) compute the votes $V_w^{(u)}(y)$ for $u \in W_I$ via (11), and set
      $$\mu_w := \mathrm{maj}_{u \in W_I}\, V_w^{(u)}(y);$$
      (ii) if $\mu_w = 1$, update $y \leftarrow y + e_w$.

(2) Return $(\mu_w)_w$.

For $k = 0$ one has $\mathcal{I}_m = \{S\}$, $W_S = W$ and $I^c = \varnothing$; the I^c-shadow projection is the identity. In this case, the only element w with $D_R(w) = I$ is the longest element $w = w_0$, and there is a single I^c-apartment, where each chamber (a coset of $W/\{e\}$) corresponds to a single group element. Step (1)(a)(i) of the decoder degenerates to a global majority of the coordinates of y, so Step (1)(a)(ii) returns μ_{w_0}, consistently with $\mathsf{C}_W(0) = \{0, \mathbb{1}_W\}$ and $e_{w_0} = \mathbb{1}_W$. This case is fully analogous to the decoder of RM codes described above.

In accordance with Remark 5.2, decoding the symbols of a fixed type I in decreasing length removes, before w is treated, every element $w' > w$ of the same type; this guarantees that the hypothesis (12) holds and lets the vote read off μ_w directly. Peeling the layer $\mathcal{I}_{m-k}$ before $\mathcal{I}_{m-k+1}$ is exactly the passage from $\mathsf{C}_W(k)$ to $\ker\phi_k = \mathsf{C}_W(k-1)$ in Theorem 3.5.

Theorem 5.3. *Let $c \in \mathsf{C}_W(r)$ and $y = c + \epsilon$ with $\mathrm{wt}(\epsilon) \le d_r/2 - 1$. Then the majority-logic decoder returns the information symbols μ_w of c; see Eq. (9).*

Proof. Put $t := \mathrm{wt}(\epsilon) \le d_r/2 - 1$, so $2t < d_r$. We show by downward induction on k that, when the outer loop reaches index k, the current word equals $y = c_k + \epsilon$, where $c_k := \sum_{w:\,|D_R(w)| \ge m-k} \mu_w e_w$ is the part of c of descent number $\ge m-k$, and that all symbols μ_w with $|D_R(w)| = m-k$ are then computed correctly.

At step k, the residual is $y = c_k + \epsilon$ (for $k = r$ this is the input $y = c + \epsilon$). Fix $I \in \mathcal{I}_{m-k}$ and process the elements w with $D_R(w) = I$ in the order of decreasing length. Suppose that the currently processed element is w, then the current residual word is $y = c' + \epsilon$, where c' is obtained from c_k by deleting every already processed symbol as in Step (1)(a)(ii). The deleted symbols are precisely the same-type elements whose lengths exceed $\ell(w)$; in particular, every w' with $D_R(w') = I$ and $w' > w$ (and thus also $\ell(w') > \ell(w)$) has been deleted, so c' satisfies (12). Moreover, $c' \in \mathsf{C}_W(k)$, so Lemma 5.1 implies that the vote value in the absence of errors is μ_w. Since

$$|W_I| \ge d_k \ge d_r > 2t \ge 2\,\mathrm{wt}(\epsilon), \tag{14}$$

the majority returns μ_w correctly. Step (1)(a)(ii) then subtracts $\mu_w e_w$, so the structure is preserved for the next step.

Once all w with $|D_R(w)| = m-k$ are processed, the residual vector is $c_{k-1} + \epsilon$, where the error ϵ is unchanged from y, so the recursion can continue. At $k = 0$ the single symbol μ_{w_0} is recovered by the global majority, again correct as above. After the loop, the residual vector is ϵ and all information symbols have been recovered. ☐

Theorem 5.3 implies that errors of multiplicity t are corrected as long as t satisfies Eq.(14). Since d_r is even, this shows that $\mathrm{dist}(\mathsf{C}_W(r)) \ge d_r - 1$, stopping one short of the exact value. The loss occurs because of the ties that can arise in the case of exactly $d_r/2$ errors; the combinatorial proof of Theorem 1.1 corresponds to error *detection* rather than correction and thus avoids this issue. Phrased differently, if the decoding algorithm is used to detect errors and returns a codeword only if all the votes agree, then to fail it needs $\mathrm{wt}(\epsilon) \ge d_r$, showing again that $\mathrm{dist}(\mathsf{C}_W(r)) = d_r$.

Remark 5.4. (The case of RM codes) The opening paragraph of this section contains an informal description of Reed's decoding of RM codes. Relying on the above discussion, we present it concisely and more formally. When $W = \mathbb{Z}_2^m$ (type mA_1), W_I is the coordinate subgroup on I, a chamber wW_{I^c} is the r-flat through w parallel to $\langle I\rangle$, and the apartment Σ_w is the partition of $\mathbb{Z}_2^m$ into the cosets of that flat. Since the flats partition the group, the retraction map is trivial, the blocks $T_w^{(u)}$ coincide with chambers, the matrix $N(w, w')$ of Lemma 5.1 is the identity, and the decreasing-length ordering is vacuous. The votes recover all degree-r coefficients in parallel, and this constitutes one step of the original Reed decoding procedure.

5.3. **Example.** Let $W = S_4, S = \{s_i = (i, i+1) : 1 \le i \le 3\}$. Consider a decoding step of the code $\mathsf{C}_{S_4}(1)$ with the parameters $[n = 24, \dim = 12, \mathrm{dist} = 4]$. We will illustrate the forming of parities for one coefficient μ_w in (9), taking $w = s_1 s_3 = 2143$ (in one-line notation). We note that the operations described below do not depend on c or on ϵ: the processing is exactly the same, and if the error weight exceeds the correction radius, the vote may return an incorrect value.

apartments / chambers	$\{1,2\}$	$\{1,3\}$	$\{1,4\}$	$\{2,3\}$	$\{2,4\}$	$\{3,4\}$
$(1,2)$	·	1342	1432	·	·	·
$(1,3)$	1243	·	1423	·	·	·
$(1,4)$	1234	1324	·	·	·	·
$(2,1)$	·	·	·	2341	2431	·
$(2,3)$	**2143**	·	·	·	2413	·
$(2,4)$	2134	·	·	2314	·	·
$(3,1)$	·	·	·	3241	·	3421
$(3,2)$	·	3142	·	·	·	3412
$(3,4)$	·	3124	·	3214	·	·
$(4,1)$	·	·	·	·	4231	4321
$(4,2)$	·	·	4132	·	·	4312
$(4,3)$	·	·	4123	·	4213	·

TABLE 1. Partition of W for the decoding of $\mu_w, w = 2143$.

Table 1 shows the partition of W for the recovery of μ_w. It depends on w through $I = D_R(w) = \{s_1, s_3\}$. We have $W_I = \langle s_1\rangle \times \langle s_3\rangle$ and $W_{I^c} = \langle s_2\rangle$, so every I-chamber uW_{I^c} contains two elements determined by the pair $(p,q) := (u(1), u(4))$, and every I-apartment is determined by four elements x that form the set $\{x(1), x(2)\}$. The rows of Table 1 show the partition of W into 12 chambers, with the pairs (p,q) as the row labels, and each column lists the four elements x indexing the same apartment, with the shared set $\{x(1), x(2)\}$ as the corresponding label.

The retraction mapping of Lemma 4.4 provides a way to assemble the votes for μ_w from the coordinates of y into the blocks $T_w^{(u)}$ as in Eq. (11). Recall that the retraction r_w centered at w is defined as $r_w(\Omega) = w\, r_0(w^{-1}\Omega)$ with $r_0(vW_{I^c}) = \beta_I(v)W_{I^c}$ for the minimal representatives $v \in W^{I^c}$. In our case, $w = w^{-1} = s_1s_3 = 2143 = (12)(34)$ (in the cycle notation), and our labelling scheme for the chambers guarantees that $w(p,q) = (w(p), w(q))$. Furthermore, if $v \in W^{I^c}$, $vW_{I^c} = (p,q)$, and $\beta_I(v)W_{I^c} = (p',q')$ (in other words, if v and $\beta_I(v)$ send $(1,4)$ to (p,q) and (p',q'), respectively, in the coordinate-wise action), then we have the following:

(a) If $p = v(1) = 1$, then v can be generated by $S \setminus \{s_1\}$, so its reduced words do not include s_1 and the same is true for $\beta_I(v)$, and therefore $p' = 1$.
(b) If $p = v(1) > 1$, then v cannot be generated by $S \setminus \{s_1\}$, so every reduced word of v includes s_1; equivalently, $s_1 \le v$ in the Bruhat order. Since $s_1 \in W_I$, the maximality of $\beta_I(v)$ in $\{u \in W_I : u \le v\}$ (Lemma 4.3) gives $s_1 \le \beta_I(v)$, so $\beta_I(v) \in \{s_1, s_1s_3\}$; in either case, $p' = 2$.

Similarly, we have $q' = 4$ if $q = u(4) = 4$ and $q' = 3$ otherwise, so we have

$$r_0((p,q)) = (p',q'), \quad \text{where } p' = 1 \text{ if } p = 1, \text{ else } 2; \text{ and } q' = 4 \text{ if } q = 4, \text{ else } 3. \tag{15}$$

It further follows that

$$r_w((p,q)) = (p'',q''), \quad \text{where } p'' = 2 \text{ if } p = 2, \text{ else } 1; \text{ and } q'' = 3 \text{ if } q = 3, \text{ else } 4. \tag{16}$$

For example, if $(p,q) = (2,1)$, then $r_w((p,q)) = (2,4)$.

We can use Eq. (16) to calculate the fibers of the retraction r_w. The outcome of these calculations is summarized in Table 2. Note that the "center" chamber $C_w := wW_{I^c}$ has preimage $r_w^{-1}(C_w) = \{C_w\}$, as promised by Lemma 4.4(c).

anchor	block (chambers)	group elements (supp(e_w) in bold)
$(2,3)$	$(2,3)$	**2143**, 2413
$(2,4)$	$(2,4),(2,1)$	**2134**, 2314, 2341, 2431
$(1,3)$	$(1,3),(4,3)$	**1243**, 1423, 4123, 4213
$(1,4)$	$(1,4),(1,2),(3,1),$	**1234**, 1324, 1342, 1432, 3241, 3421, 3142,
	$(3,2),(3,4),(4,1),(4,2)$	3412, 3124, 3214, 4231, 4321, 4132, 4312

Table 2. The votes table for the coefficient $\mu_{w=(2143)}$. The elements in the support of e_w, i.e., the elements of wW_I, are typeset in boldface. Anchors refer to the chambers that contain those elements.

Remark 5.5. For better readability, we chose $W_I = \langle s_1, s_3\rangle$ with commuting generators, resulting in $|W_I| = 4$. For the case of non-commuting generators, we could take $I = \{s_1, s_2\}$, then apartments become hexagons rather than squares, every pair of apartments share 2 chambers (apartments glue along edges), the retraction does not factor because β_I is a genuine Demazure product on $\{s_1, s_2\}$-words, and the forming of the blocks $T_w^{(u)}$ depends on the choice of the direction (s_1 or s_2).

6. Concluding remarks

General Coxeter codes are defined in combinatorial-geometric terms as in Eq. (9). RM codes, in addition, can be described relying on polynomial formalism as discussed at the beginning of Sec. 5. It is not clear to us whether the polynomial description affords a well-formed extension to the case of general (finite) Coxeter groups.

In [5, App. B], Coble defines the so-called subapartment codes and residue codes, which are two kinds of building-theoretic extensions of Coxeter codes. By definition, a subapartment code is the span of the indicator vectors of subapartments of rank $m - r$ in a finite spherical building of rank m, whereas residue codes are spanned by the indicator vectors of residues of rank $m - r$. When the building is the Coxeter complex of (W, S), these two definitions recover the Coxeter code $C_W(r)$. This suggests several natural questions beyond the finite Coxeter-group setting. The most immediate questions concern the basic coding-theoretic parameters: determining the dimension and minimum distance of these building codes. It would also be interesting to understand whether the shadow-code and rank-selected retraction methods used here have analogues and whether they can be used to prove dimension or distance statements in this more general setting.

7. Acknowledgments

The authors are grateful to Myna Vajha for suggesting exploring links between a majority-logic decoder of Coxeter codes and the minimum distance conjecture, and to James Davis for helpful discussions. A.B. was supported in part by NSF grants CCF-2330909 and CCF-2526035; T.X. was supported in part by an AMS–Simons Research Enhancement Grant for PUI Faculty. This project was initiated while the authors took part in the workshop "The Interplay Between Distance Geometry, Combinatorics, and Coding Theory" organized at the Brin Mathematics Research Center at the University of Maryland, College Park, in November 2025. The authors used large language models, including ChatGPT-5.4 and Claude Sonnet 4.6, as exploratory tools in connection with the problem studied in this paper. Their use was limited to brainstorming, discussion of possible approaches, and preliminary checking of ideas. All mathematical arguments were independently written by the authors, who take full responsibility for the content of the paper.

References

[1] E. Abbe, O. Sberlo, A. Shpilka, and M. Ye. Reed-Muller codes. *Foundations and Trends in Communications and Information Theory*, 20(1–2):1–156, 2023.

[2] E. F. Assmus, Jr. and J. D. Key. Polynomial codes and finite geometries. In *Handbook of Coding Theory*, volume II, pages 1269–1343. North-Holland, Amsterdam, 1998.

[3] A. Barg, N. J. Coble, D. Hangleiter, and C. Kang. Geometric structure and transversal logic of quantum Reed–Muller codes. *IEEE Transactions on Information Theory*, 72:415–436, 2026.

[4] A. Björner and F. Brenti. *Combinatorics of Coxeter Groups*. Graduate texts in mathematics. Springer, New York, 2005.

[5] N. J. Coble. *New directions from old codes*. PhD thesis, University of Maryland, 2025. http://hdl.handle.net/1903/35112.

[6] N. J. Coble and A. Barg. Coxeter codes: extending the Reed–Muller family. *Designs, Codes and Cryptography*, 94(2):47, 2026.

[7] M. Demazure. Désingularisation des variétés de Schubert généralisées. *Annales scientifiques de l'École Normale Supérieure*, 4e série, 7(1):53–88, 1974.

[8] D. Jahn and C. Stump. Bruhat intervals, subword complexes and brick polyhedra for finite Coxeter groups. *Math. Z.*, 304(24), 2023.

[9] A. Knutson and E. Miller. Subword complexes in Coxeter groups. *Advances in Mathematics*, 184(1):161–176, 2004.

[10] F. J. MacWilliams and N. J. A. Sloane. *The Theory of Error-Correcting Codes*. North-Holland Pub. Co., Amsterdam; New York, N.Y., 1977.

[11] D. E. Muller. Application of Boolean algebra to switching circuit design and to error detection. *Transactions of the IRE Professional Group on Electronic Computers*, EC-3(3):6–12, 1954.

[12] I. Reed. A class of multiple-error-correcting codes and the decoding scheme. *IEEE Trans. Inform. Theory*, 4:38–49, 1954.

University of Maryland, College Park, MD 20817, USA
Email address: `abarg@umd.edu`

University of Maryland, College Park, MD 20817, USA & University of Prishtina, Kosovo
Email address: `qgashi@umd.edu`

University of Richmond, Richmond, VA 23173, USA
Email address: `txu@richmond.edu`