Master thesis

The Stabilizer Polytope and Contextuality for Qubit Systems

Arne Heimendahl

University of Cologne

supervised by
Prof. Dr. Frank Vallentin, Prof. Dr. David Gross

June 4, 2019

Acknowledgments

First, I would like to thank my thesis advisors Frank Vallentin and David Gross. They encouraged me enormously and provided me with a thrilling topic that caught my attention far beyond the scope of this thesis. Moreover, many thanks to Markus and Felipe for a lot of helpful discussions and ideas, as well as to Felix for proofreading and to Maxi for extensive help with the figures.

I would like to express my thankfulness to my parents for their unconditional support during my whole studies. Of course, I will not forget to mention the other fellow students and friends who made the last years such a wonderful time for me!

Contents

Chapter 1

Introduction

Quantum algorithms are able to solve certain problems essentially faster than current state-of-the-art classical algorithms, the main example being Shor's factoring algorithm [1]. In order to use the theoretical computational power of a quantum computer, mathematical frameworks are required that guarantee a high level of fault-tolerance. Additionally, they have to ensure the ability to *universal quantum computation* meaning that any operation that we can theoretically perform with a quantum computer is realizable within this framework.

The *stabilizer framework* seems promising to achieve this goal [2]- however, it can be seen as a closed subtheory of quantum theory which is not universal and its computational power is restricted due to the Gottesman-Knill theorem [3]. In fact, we can efficiently simulate the outcomes of a circuit based on stabilizer operations with a classical computer.

Fortunately, we can promote the stabilizer framework to universality by a process called *magic state distillation*, originally proposed by Bravyi and Kitaev [4]. Loosely speaking, we effectuate a non-stabilizer operation by injecting a *magic state* into our circuit enabling us to do any operation which we can theoretically realize with a quantum computer, up to high precision.

One crucial feature of magic states is that they lie outside the *stabilizer polytope* lying at the core of the stabilizer framework. This thesis will be devoted to take a closer look at this polytope for qubit systems from a geometric point of view. We will characterize the integral points of its polar dual polytope linearly embedded in the real Euclidean space and we will prove that certain of these points will give rise to facets of the stabilizer polytope.

Besides, we will build a connection between (non-)contextuality and the integral points of the polar dual polytope. Contextuality is a feature that divides classical from quantum mechanics and such a connection has been shown to be a necessary resource for quantum computation with magic states [5][6]. As one of the main results we will characterize state independent contextuality as a violation of a facet inequality of the polar dual stabilizer polytope.

The first chapter includes a short introduction to the basic properties of polytopes which will

be frequently used in the second chapter. Moreover, we will explain all concepts of quantum information theory required for this work.

The second chapter deals with the stabilizer polytope and contextuality. In the first part we will introduce a family of lattice polytopes and analyze some of their characteristics. Particularly, we will characterize all integral points in the corresponding family of dual polytopes and show that some of these integral points give rise to facets. Embedded in the real Euclidean space, the stabilizer polytope can be classified as a member of this family.

In the second part of the chapter we will establish the connection between the stabilizer polytope and (non)-contextuality. We will use the results of the first part to deduce a geometric characterization of contextuality related to projections of the stabilizer polytope.

Chapter 2

Preliminaries

2.1 On polytopes

This section gives a shorthand introduction to the basic structural properties of polytopes, which will be frequently applied in the subsequent parts of this work. The ideas are based on the first two chapters of [7]. Detailed proofs can be found there as well.

Basic properties

Let V be a vector space over the real numbers $\mathbb{R}$ and V^* its dual space, i.e., the set of linear functionals $\ell : V \to \mathbb{R}$. A *polytope* P is defined as the convex hull of finitely many points in V meaning that there are $N \in \mathbb{N}$ and $v_1, ..., v_N \in V$ such that

$$P = \text{conv}\{v_1, ..., v_N\}.$$

Such a description is referred to as a *V-description* of P. For $\ell \in V^*$, $\beta \in \mathbb{R}$ the sets $\{x \in V \,|\, \ell(x) \leq \beta\}$ and $\{x \in V \,|\, \ell(x) \geq \beta\}$ are called *(closed) half-space*. As a consequence of the theorem of Minkowski-Weyl, polytopes are bounded polyhedra, hence, we can write them as the intersection of half-space:

$$P = \{x \in V \,|\, \ell_i(x) \leq \beta_i,\, i = 1, ..., m\}$$

for linear functionals $\ell_1, ..., \ell_m \in V^*$. Such a description is called an *H-description* of P.

The dimension of a polytope is the dimension of its affine hull i.e., $\dim P = \dim(\text{aff}(P))$. We call a polytope $P \subset V$ *full-dimensional* if $\dim P = \dim V$. Note that P is full-dimensional iff there is a point x lying in the interior of P (which we will denote by $\text{int}(P)$).

Particularly, we are interested in the structure of the boundary of a polytope. If P is a polytope, then $F \subseteq P$ is called a *face* of P if there is an affine subspace $H = \{x \in V \,|\, \ell(x) = \beta\}$ such that $F = \{x \in P \,|\, \ell(x) = \beta\}$ and $P \subset \{x \in V \,|\, \ell(x) \leq \beta\}$. If we set $\ell \equiv 0$ and $\beta = 1$, respectively $\beta = -1$, we see that P, respectively $\emptyset$ are faces of P. All other faces $F \neq P, \emptyset$ are called *proper faces*.

The dimension of a face is the dimension of its affine hull, i.e., $\dim F = \dim(\text{aff}(F))$. Zero-dimensional faces are called *vertices*, 1-dimensional faces *edges* and faces of dimension $\dim(P)-1$ *facets*. The set of vertices of a polytope P will be denoted by $\mathcal{V}(P)$. We will state some basic properties of faces.

Proposition 2.1.1. *Let $P \subset V$ be a polytope and let F be a face of P.*

(i) F is a polytope and $\mathcal{V}(F) = F \cap \mathcal{V}(P)$.

(ii) The intersection of faces of P is a face of P.

(iii) The faces of F are exactly the faces of P that are contained in F.

(iv) $F = P \cap \text{aff}(F)$.

If we are given an H-description of a polytope, we are often interested in an "irreducible" description, i.e., we do not want to list inequalities that hold for P but are already implied by other inequalities holding for P. An H-description $P = \{x \in V \,|\, \ell_i(x) \leq \beta_i,\, i = 1, ..., m\}$ of a polytope P is *non-redundant* if the sets $\{x \in P \,|\, \ell_i(x) = \beta_i\}$ are facets of P for all $i = 1, ..., m$. This is equivalent to $\{x \in V \,|\, \ell_i(x) \leq \beta_i,\, i \in I \subsetneq \{1, ..., m\}\} \neq P$ for all proper subsets I of $\{1, ..., m\}$. This means that we cannot remove inequalities form the H-description without changing the set P. If P is full-dimensional, a non-redundant H-description is unique up to multiples $\alpha\ell(x) \geq \alpha\beta$ with $\alpha > 0$. Every proper face of P can be seen as the intersection of facets, thus, for every proper face F of P there exists a set $I \subset \{1, ..., m\}$ such that $F = \{x \in P \,|\, \ell_i(x) \leq \beta_i \text{ for all } i \in I\}$.

If a polytope P is given by its H-description, there are several equivalent characterizations of its vertices (or 0-faces):

Proposition 2.1.2. *Let $P = \{x \in V \,|\, \ell_i(x) \leq \beta_i,\, i = 1, ..., m\} \subset V$ be a polytope and $v \in P$. Then the following properties of v are equivalent:*

(i) v is a vertex of P.

(ii) If $v = \lambda v_1 + (1-\lambda)v_2$ for $0 \leq \lambda \leq 1$ and $v_1, v_2 \in P$, then $v = v_1 = v_2$. Since this is the (general) definition of an extreme point, v is an extreme point of P.

(iii) $\dim\left(\text{span}\{\ell_i \,|\, \ell_i(v) = \beta_i,\, i \in \{1, ..., m\}\}\right) = \dim V^* = \dim V$.

(iv) There exists $\ell \in V^*$ such that $\ell(v) > \ell(x)$ for all $x \in P \setminus \{v\}$.

A proof can be found in [8, Section 2.2]. There is also a useful characterization for faces of dimension 1, i.e., the edges. For two points $v_1, v_2 \in V$ we define the line segment between v_1 and v_2 as

$$[v_1, v_2] := \{\lambda v_1 + (1-\lambda)v_2 \,|\, 0 \leq \lambda \leq 1\}.$$

Proposition 2.1.3. *Let $P \subset V$ be a polytope and $v_1, v_2 \in \mathcal{V}(P)$. The line segment $[v_1, v_2]$ is an edge of P if and only if there is an $\ell \in V^*$ such that $\ell(v_1) = \ell(v_2)$ and $\ell(v) < \ell(v_1)$ for all $v \in \mathcal{V}(P) \setminus \{v_1, v_2\}$.*

The polar dual polytope

Let $M \subset V$. The *polar set* of M is given by

$$M^\circ = \{\ell \in V^* \,|\, \ell(x) \geq -1 \text{ for all } x \in M\}.$$

Note that this definition varies from the usual definition of the polar set in the literature because one usually demands $\ell(x) \geq 1$. This coincides with the set $-M^\circ$ in our context. Yet, for the purpose of this thesis it is more convenient to demand $\ell(x) \geq -1$. The set M° is convex independently of the shape of M, as the intersection of (infinitely) many half-space. Moreover, if $M \subset M'$, then clearly $(M')^\circ \subset M^\circ$. For example, if $B(0,r) = \{x \in V \,|\, \|x\| \leq r\}$ is the ball of radius $r > 0$ then $B(0,r)^\circ = B(0,1/r)$ is the ball of radius $1/r$.

If P is a polytope, then P° is a polytope as well under certain circumstances. Additionally, there is a strong relation between the facets of P and the vertices of P° (in general, there is a strong relation between their face lattices, for further details see [7]).

Lemma 2.1.4. *Let $P = \text{conv}\{v_1, ..., v_N\}$ be a full-dimensional polytope with $0 \in \text{int}(P)$. Then P° is a full-dimensional polytope with $0 \in V^*$ in the interior of P° and*

$$P^\circ = \{\ell \in V^* \,|\, \ell(v_i) \geq -1 \text{ for all } i = 1, ..., N\},$$

where the sets $\{\ \ell \in P^\circ \,|\, \ell(v_i) = -1\ \}$ are facets of P° for all $i = 1, ..., N$. Moreover, it holds $(P^\circ)^\circ = P$.

The lemma has the following consequence: If P is full-dimensional with $0 \in \text{int}(P)$ and dual polytope P° with vertex set $\mathcal{V}(P^\circ) = \{\ell_1, ..., \ell_m\}$, then a non-redundant H-description of P is given by $P = \{x \in V \,|\, \ell_i(x) \geq -1,\ i = 1, ..., m\}$.

Lattice polytopes

We set $V = \mathbb{R}^d$ and fix the lattice $\mathbb{Z}^d \subset \mathbb{R}^d$. A polytope P is called a *lattice polytope* (or *integral*) if $\mathcal{V}(P) \subset \mathbb{Z}^d$. Lattice polytopes are especially interesting in optimization since determining the maximum of linear function over all lattice points in a polytope (which is known as integer programming and is NP-complete in general) boils down to maximizing the linear function over the whole polytope (which can be solved in polynomial time and is known as linear programming).

Every linear functional $\ell \in (\mathbb{R}^d)^*$ can be written as $\ell(x) = a^T x$ for some $a \in \mathbb{R}^d$, so we can identify $(\mathbb{R}^d)^*$ with $\mathbb{R}^d$. Let P be a full-dimensional lattice polytope with $0 \in \text{int}(P)$. Then P is *reflexive* if P° is also a lattice polytope, i.e., $\mathcal{V}(P^\circ) \subset \mathbb{Z}^d$. The most common example is the hypercube $C_d = \text{conv}\{v \,|\, v \in \{-1, 1\}^d\}$ with its dual polytope $(C_d)^\circ = \text{conv}\{\pm e_i,\ i = 1, ..., d\}$ where $e_1, ..., e_d$ is the standard basis of $\mathbb{R}^d$. In Section 3.1 we will see another family of reflexive polytopes (where some of them are even *self-dual*, i.e., $P = P^\circ$) as projections of the stabilizer polytope.

2.2 Quantum information theory

The foundational objects in quantum information theory are complex matrices. We will briefly introduce the ones which will appear in this thesis. A matrix $A \in \mathbb{C}^{d\times d}$ is called *Hermitian* if $A = A^\dagger$, where the entry $A^\dagger_{ij}$ is the complex conjugate of the entry A_{ji}, i.e., $A^\dagger_{ij} = \overline{A_{ji}}$ for all $i, j \in \{1, ...d\}$. We call a matrix A *Hermitian positive semidefinite* (shortly psd) if A is Hermitian and $x^\dagger Ax \geq 0$ for all $x \in \mathbb{C}^d$. A *state* ρ is a Hermitian positive semidefinite matrix that additionally satisfies $\mathrm{Tr}(\rho) = 1$. A matrix U is *unitary* if $UU^\dagger = I$, where I denotes the identity matrix. Note that if U is unitary and ρ a state then $U\rho U^\dagger$ remains a state.

Oftentimes, the matrices act on the tensor space $(\mathbb{C}^2)^{\otimes n} \cong \mathbb{C}^{2^n}$ (where $\otimes$ is the standard symbol for tensor products). Vectors in $\mathbb{C}^{2^n}$ will be denoted in the bra-ket notation, i.e., we will write $|\psi\rangle \in \mathbb{C}^{2^n}$ and $\langle\psi|$ for the conjugate transpose.

If $A \in \mathbb{C}^{2\times 2}$ and if not defined specifically in another manner, then $A_i \in \mathbb{C}^{2^n\times 2^n}$ for $i \in \{1, ..., n\}$ represents the matrix

$$A_i = \underbrace{I \otimes \cdots I}_{(i-1)-\text{times}} \otimes A \otimes \underbrace{I \otimes \cdots \otimes I}_{(n-i)-\text{times}}, \tag{2.1}$$

i.e., the matrix A_i sits at the $i-$th tensor. If $|\psi\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle \in \mathbb{C}^{2^n}$, then

$$A_i |\psi\rangle = A_i |\psi_1\rangle \otimes \cdots \otimes |\psi_n\rangle = |\psi_1\rangle \otimes \cdots \otimes |\psi_{i-1}\rangle \otimes A|\psi_i\rangle \otimes |\psi_{i+1}\rangle \otimes \cdots \otimes |\psi_n\rangle,$$

so A_i acts on the i-th qubit of $|\psi\rangle$ and leaves the remaining qubits invariant.

The $n-$qubit Pauli group and stabilizer codes

In this section we introduce the basic objects of the *stabilizer formalism*. This closed subtheory of quantum computation has proved to be extremely useful to design a mathematical basis for fault tolerant quantum computation as it allows a high degree of quantum error correction [2].

The section is based on the ideas and notion of chapter 10 of the textbook [9]. Let

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

be the Pauli X, Y and Z matrices. If we consider the vector space of 2×2 Hermitian matrices as a 4-dimensional real valued vector space, X, Y, Z together with the identity matrix $I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ form an orthogonal basis for this space with respect to the trace inner product. The set of n-fold tensors of Pauli matrices is defined as

$$P_n = \left\{ \bigotimes_{i=1}^{n} W_i \,|\, W_i \in \{I, X, Y, Z\} \right\}$$

and is a basis for the real valued 4^n-dimensional vector space of $2^n \times 2^n$ Hermitian matrices. Using the notation of (2.1) we can write this as

$$\left\{ \prod_{i=1}^{n} A_i^{(i)} \mid A_i^{(i)} \in \mathbb{C}^{2^n \times 2^n},\, A^{(i)} \in \{I, X, Y, Z\} \right\},$$

e.g., we will write $X_1 Y_3 \in P_3$ for $X \otimes I \otimes Y$. In slight abuse of notation, we use the symbol I for the identity matrix of arbitrary dimension if it does not cause any ambiguities. Some important properties of elements in P_n are listed below:

(i) They are all unitary and Hermitian, thus $g^2 = I$ for all $g \in P_n$.

(ii) The eigenvalues are $+1$ and -1 and the projectors onto the eigenspaces are $(I+g)/2$ for the $+1$ eigenspace, respectively $(I-g)/2$ for the -1 eigenspace. This can be easily seen since for a vector $|\psi\rangle \in (\mathbb{C}^2)^{\otimes n}$

$$g\left(\frac{I+g}{2}|\psi\rangle\right) = \frac{g+g^2}{2}|\psi\rangle = \frac{I+g}{2}|\psi\rangle$$

and we can argue analogously for the projector onto the -1 eigenspace.

(iii) Two matrices in P_n either commute or anticommute, that is $gg' = g'g$ or $gg' = -g'g$ for any $g, g' \in P_n$.

	X	Y	Z
X	I	iZ	iY
Y	$-iZ$	I	iX
Z	$-iY$	$-iX$	I

Figure 2.1: Multiplication table for the Pauli matrices where we multiply row times column.

Adding a global phase $\pm 1, \pm i$ to the operators in P_n we define the union

$$\mathcal{P}_n = P_n \cup -P_n \cup iP_n \cup -iP_n,$$

which is closed under multiplication and forms a multiplicative group, the *Pauli group* with center $Z(\mathcal{P}_n) = \{\pm I^{\otimes n}, \pm iI^{\otimes n}\}$. The set $P_n \cup -P_n$ will be denoted by $\pm P_n$ and sometimes we will refer to elements in $\mathcal{P}_n$ as *Pauli observables*.

We define the function $\chi : \mathcal{P}_n \to \{\pm 1, \pm i\}$ where $\chi(g)$ is the global phase of $g \in \mathcal{P}_n$, i.e., if $g \in \omega P_n$ for $\omega \in \{\pm 1, \pm i\}$, then $\chi(g) = \omega$. The function satisfies $\chi(\omega g) = \omega \cdot \chi(g)$ for $\omega \in \{\pm 1, \pm i\}$ but it is worth to mention that χ is not multiplicative, e.g., $\chi(X_1X_2) = \chi(Y_1Y_2) = 1$ but $\chi((X_1X_2)(Y_1Y_2)) = \chi(-Z_1Z_2) = -1$.

We are especially interested in commuting subgroups of $\mathcal{P}_n$. A crucial observation is that $(\mathcal{P}_n/Z(\mathcal{P}_n), \cdot) \cong (\mathbb{F}_2^n, +)$ where $\mathbb{F}_2 \cong \mathbb{Z}_2$ is the unique field with characteristic 2. We will also

refer to $\mathbb{F}_2^{2n}$ as the *phase space*. Certain properties of $\mathbb{F}_2^{2n}$ are discussed in more detail in the subsection about *isotropic subspaces of* $\mathbb{F}_2^{2n}$.

The quotient group $\mathcal{P}_n/Z(\mathcal{P}_n)$ is generated by the cosets $[X_1], ..., [X_n], [Z_1], ..., [Z_n]$. Now, the isomorphism is realized by mapping $[X_i]$ to u_i and $[Z_i]$ to v_i, where

$$u_i(j) = \begin{cases} 1, \text{ if } i = j, \\ 0, \text{otherwise}, \end{cases} \qquad v_i(j) = \begin{cases} 1, \text{ if } i = n + i \\ 0, \text{ otherwise.} \end{cases}$$

For the case $n = 1$ the isomorphism is realized via the identification

$$X \mapsto (0, 1),\ Y \mapsto (1, 1),\ Z \mapsto (1, 0).$$

We define $r : \mathcal{P}_n \to \mathbb{F}_2^{2n}$ as the binary representation of elements $g \in \mathcal{P}_n$, where for $g \in \mathcal{P}_n$ the image $r(g)$ is the image of the coset $[g]$ under the isomorphism to $\mathbb{F}_2^{2n}$. Note that r is a surjective homomorphism. Since $r(g) = r(-g) = r(ig) = r(-ig)$ for all $g \in P_n$, the homomorphism has the following property

$$|r^{-1}(h) \cap \omega P_n| = 1 \tag{2.2}$$

for all $h \in \mathbb{F}_2^{2n}$ and $\omega \in \{\pm 1, \pm i\}$. For a Pauli matrix $A_i \in P_n$ with $A \in \{X, Y, Z\}$ acting on the $i - th$ qubit we will use small letters if we want to refer to its representation in the phase space, i.e., we set $r(A_i) := a_i$. If we have a matrix $A \in P_n$ acting on k qubits, i.e., $A := A_{i_1}^{(1)} A_{i_2}^{(2)} \cdots A_{i_k}^{(k)} \in P_n$ with $A^{(j)} \in \{X, Y, Z\}$ for $j = 1, ..., k$ and $i_1 < i_2 < \cdots < i_k$, we will set $r(A) := a_{i_1} \cdots a_{i_k}$, for instance $r(X_1 Y_3) = x_1 y_3$.

Additionally, we equip $\mathbb{F}_2^{2n}$ with a symplectic inner product, that is for $h_1 = (u_1, v_1), h_2 = (u_2, v_2) \in \mathbb{F}_2^{2n}$ we define

$$h_1 \cdot h_2 = u_1^T v_2 + u_2^T v_1 = h_1^T \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} h_2,$$

where I denotes the $n \times n$ identity matrix. As we will see in the sequel commutativity in $\mathcal{P}_n$ is equivalent to orthogonality in $\mathbb{F}_2^{2n}$. For $g_1, g_2 \in P_n$ we want to construct a function $f : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{C}$ such that f keeps track of the global phase of $g_1 g_2$, i.e., we want that $\chi(g_1 g_2) = f(r(g_1), r(g_2))$. Our idea is similar to [10] where all actions on stabilizer groups are described by binary linear and quadratic operations. The specific choice of f is constructed as follows:
For $h_1 = (u_1, v_1)$, $h_2 = (u_2, v_2) \in \mathbb{F}_2^{2n}$ we define

$$f : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{C}, \quad f(h_1, h_2) = (-i)^{(u_1^T v_2)} \cdot i^{(u_2^T v_1)}. \tag{2.3}$$

We will state some properties of f:

Proposition 2.2.1. *(i) The evaluation $f(r(g_1), r(g_2))$ for $g_1, g_2 \in P_n$ coincides with the*

global phase of the product $g_1 g_2 \in \pm P_n$, that is, if $\chi(g_1) = \chi(g_2) = 1$, then $\chi(g_1 g_2) = f(r(g_1), r(g_2))$.

(ii) f is bilinear, that is $f(h_1, h_2 + h_3) = f(h_1, h_2) f(h_1, h_3)$ as well as $f(h_1 + h_2, h_3) = f(h_1, h_3) f(h_2, h_3)$ for all $h_1, h_2, h_3 \in \mathbb{F}_2^{2n}$.

(iii) f is symmetric for orthogonal elements and antisymmetric for non-orthogonal ones, more precisely $f(h_1, h_2) = f(h_2, h_1) \in \{1, -1\}$ if $h_1 \cdot h_2 = 0$ and $f(h_1, h_2) = -f(h_2, h_1) \in \{i, -i\}$ if $h_1 \cdot h_2 = 1$.

Since every element in $\mathcal{P}_n$ can be written as ωg where $\omega \in \{1, -1, i, -i\}$, $g \in P_n$ and $\chi(\omega g) = \omega$, property (i) can be extended to Pauli matrices with arbitrary phase as follows: Let $\omega_1 g_1$, $\omega_2 g_2 \in \mathcal{P}_n$ where $\omega_1, \omega_2 \in \{1, -1, i, -i\}$ and $g_1, g_2 \in P_n$, then

$$\begin{aligned} \chi(\omega_1 g_1 \cdot \omega_2 g_2) &= \omega_1 \cdot \omega_2 \cdot f(r(g_1), r(g_2)) \\ &= \chi(\omega_1 g_1) \cdot \chi(\omega_1 g_1) \cdot f(r(g_1), r(g_2)). \end{aligned} \tag{2.4}$$

Proof. (i) We can easily verify that the statement is true for $n = 1$. Recall that $r(I) = (0, 0)$, $r(X_1) = x_1 = (1, 0)$, $r(Z_1) = z_1 = (0, 1)$ and $r(Y_1) = y_1 = (1, 1)$. To check the case $n = 1$ it suffices to evaluate f for these points and then do a parity check with the global phases of Table 2.1 in the preliminaries.
Now, let $n \geq 1$ and $g_1 = \bigotimes_{k=1}^n W_k^{(1)}$, $g_2 = \bigotimes_{k=1}^n W_k^{(2)} \in \mathcal{P}_n$ where $W_k^{(1)}, W_k^{(2)} \in \{I, X, Y, Z\}$ for $k = 1, ..., n$. By construction, $\chi(g_i) = 1$ for $i = 1, 2$. Moreover, let $r(g_i) = (u_i, v_i) \in \mathbb{F}_2^{2n}$ the representation of g_i in the phase space with $(u_i(k), v_i(k)) = r(W_k^{(i)})$ for $i = 1, 2$. Then

$$\begin{aligned} \chi(g_1 g_2) = \chi\left(\bigotimes_{k=1}^n W_i U_i\right) = \prod_{k=1}^n \chi(W_i U_i) &= \prod_{k=1}^n \left((-i)^{u_1(k) v_2(k)} \cdot i^{u_2(k) v_1(k)}\right) \\ &= \prod_{k=1}^n (-i)^{u_1(k) v_2(k)} \prod_{k=1}^n i^{u_2(k) v_1(k)} \\ &= (-i)^{(u_1^T v_2)} \cdot i^{(u_2^T v_1)} \\ &= f(r(g_1), r(g_2)), \end{aligned}$$

which shows the desired property for any n.

(ii) Let $h_i = (u_i, v_i) \in \mathbb{F}_2^{2n}$ for $i = 1, 2, 3$. We can directly verify

$$\begin{aligned} f(h_1, h_2 + h_3) = (-i)^{u_1^T (v_2 + v_3)} \cdot i^{(u_2 + u_3)^T v_1} &= \left((-i)^{u_1^T v_2} \cdot i^{u_2^T v_1}\right) \cdot \left((-i)^{u_1^T v_3} \cdot i^{u_3^T v_1}\right) \\ &= f(h_1, h_2) f(h_1, h_3) \end{aligned}$$

and $f(h_1 + h_2, h_3) = f(h_1, h_3) f(h_2, h_3)$ follows analogously.

(iii) Let $h_1 = (u_1, v_1)$, $h_2 = (u_2, v_2) \in \mathbb{F}_2^{2n}$. The crucial step is to rewrite $f(h_1, h_2)$ as

$$f(h_1, h_2) = (-1)^{(u_1^T v_2)} \cdot i^{(u_1^T v_2 + u_2^T v_1)}.$$

Observing that $h_1 \cdot h_2 = u_1^T v_2 + u_2^T v_1 \pmod 2$ we have $f(h_1, h_2) \in \{1, -1\}$ if $h_1 \cdot h_2 = 0$ and $f(h_1, h_2) \in \{i, -i\}$ if $h_1 \cdot h_2 = 1$. To show symmetry, respectively antisymmetry, it suffices to note that $u_1^T v_2 \,(\mathrm{mod}\, 2) = u_2^T v_1 \,(\mathrm{mod}\, 2)$ if $h_1 \cdot h_2 = 0$ and $u_1^T v_2 \pmod 2 \neq u_2^T v_1 \pmod 2$ if $h_1 \cdot h_2 = 1$, Hence, we have

$$f(h_1, h_2) = (-1)^{(u_1^T v_2)} i^{(u_1^T v_2 + u_2^T v_1)} = (-1)^{(u_2^T v_1)} i^{(u_1^T v_2 + u_2^T v_1)} = f(h_2, h_1)$$

for $h_1 \cdot h_2 = 0$ and the case $f(h_1, h_2) = -f(h_2, h_1)$ for $h_1 \cdot h_2 = 1$ follows in the same fashion.

□

Due to the last proposition we have the following property:

Proposition 2.2.2. *It holds $g_1 g_2 = g_2 g_1$ for $g_1, g_2 \in \mathcal{P}_n$ if and only if $r(g_1) \cdot r(g_2) = 0$.*

Proof. As the global phase does not affect commutativity it suffices to show the statement for $g_1, g_2 \in P_n$. Since two Pauli matrices either commute or anticommute, $g_1 g_2 = g_2 g_1$ is equivalent to $\chi(g_1 g_2) = \chi(g_2 g_1)$. Due to (iii) of the last proposition $f(r(g_1), r(g_2)) = \chi(g_1 g_2) = \chi(g_2 g_1) = f(r(g_2), r(g_1))$ implies $r(g_1) \cdot r(g_2) = 0$. Analogously, $\chi(g_1 g_2) = -\chi(g_2 g_1)$ implies $r(g_1) \cdot r(g_2) = 1$ and the statement follows. □

Definition 2.2.3. Let $S \subset \mathcal{P}_n$ be an abelian subgroup of $\mathcal{P}_n$ and define $V_S := \{|\psi\rangle \mid g\,|\psi\rangle = |\psi\rangle \text{ for all } g \in S\}$ as the subspace, which is invariant under operations from S. The set V_S is called a *stabilizer code* fixed by the *stabilizer* S.

Note that if $g, g' \in S$ anticommute and $\psi \in S$ then

$$|\psi\rangle = gg'\,|\psi\rangle = -g'g\,|\psi\rangle = -\,|\psi\rangle$$

forces $V_S = \{0\}$. Moreover, if an element $g \in S$ has global phase $\pm i$, then $S \ni g^2 = -I$, then $V_S = \{0\}$, as well. Thus, we may restrict our attention to abelian subgroups $S \subset \pm P_n \setminus \{-I\}$. So, when talking about abelian subgroups $S \subset \pm P_n$ we always assume $-I \notin S$.

The binary representation $r(S)$ of an abelian subgroup S forms a self-orthogonal additive subgroup of the vector space $\mathbb{F}_2^{2n}$ which itself is a classical code over $\mathbb{F}_2$. This motivates the alternative term *additive code* for a stabilizer code [11].

It will be helpful to characterize the dimension of the code space V_S. Let $S = \langle g_1, \dots g_k \rangle \subset \mathcal{P}_n$ be the subgroup generated by the elements $g_1, \dots g_k$. We are interested in minimal generating sets for subgroups. Observing that $g \in \langle g_1, \dots g_k \rangle$ then $r(g) \in \mathrm{span}\{r(g_1), ..., r(g_k)\}$ we can reduce this question to find a basis of $r(S)$.

Theorem 2.2.4. *Let $S = \langle g_1, \ldots, g_{n-k} \rangle \subset \pm P_n$ be an abelian subgroup such that $-I \notin S$ and $r(g_1), \ldots, r(g_{n-k})$ are linearly independent. Then V_S is a 2^k-dimensional vector subspace.*

In this case we say that S *defines an* $[n, k]$ *stabilizer code.* We set

$$P_S := \prod_{i=1}^{n-k} \frac{(I + g_i)}{2} = \frac{1}{2^{n-k}} \sum_{g \in S} g = \frac{1}{2^{|S|}} \sum_{g \in S} g, \tag{2.5}$$

which is projector onto the common $+1$ eigenspace of the elements in S, thus it is the projector onto the code space V_S. We will prove that $\dim V_S = 2^k$ in Section 3.3.

Example 2.2.5 Let $S = \langle X_1X_2,\, Z_1Z_2 \rangle = \{X_1X_2,\, Z_1Z_2,\, -Y_1Y_2,\, I\} \subset \pm P_2$. The corresponding vectors $r(X_1X_2) = x_1x_2 = (1, 1, 0, 0)$ and $r(Z_1Z_2) = z_1z_2 = (0, 0, 1, 1)$ are linearly independent. We have

$$P_S = \frac{1}{2^2} \left(1 \cdot I + 1 \cdot X_1X_2 + 1 \cdot Y_1Y_2 + (-1) \cdot Z_1Z_2\right).$$

Since $\dim V_S = 1$, it stabilizes a single state, that is $|\psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$, hence we have $P_S = |\psi\rangle \langle\psi|$.

The stabilizer polytope

If an abelian subgroup $S \subset \pm P_n \backslash \{-I\}$ contains 2^n elements (which is equivalent to $\dim(r(S)) = n$), the matrices in S stabilize a single state $|\psi\rangle$ due to Theorem 2.2.4. Thus, P_S is a rank one projector and we can write $P_S = \frac{1}{2^n} \sum_{g \in S} g = |\psi\rangle \langle\psi|$. The state $|\psi\rangle$ is referred to as a *stabilizer state* and the polytope

$$SP_n := \mathrm{conv}\{|\psi\rangle \langle\psi| \mid |\psi\rangle \text{ stabilizer state } \}$$

is called the *stabilizer polytope*. Stabilizer states are one of the main objects used in the stabilizer formalism. The advantage of circuits based on this framework is that they allow a high degree of fault tolerance (for details see [2] and [9, Chapter 10]). However, these circuits do not have the full computational power that quantum circuits provide in general. We say that the do not allow *universal quantum comutation* (UQC).

Theorem 2.2.6 (Gottesman-Knill theorem, [3], 1998)**.** *Quantum circuits consisting of preparing stabilizer states, Clifford unitaries (this is the group of unitary matrices that normalizes the Pauli group $\mathcal{P}_n$, i.e., C is Clifford if $CgC^\dagger \in \mathcal{P}_n$ for all $g \in \mathcal{P}_n$), and measurements of Pauli observables can be efficiently simulated on a classical computer.*

The assumptions of the theorem can be extended to the preparation of a state ρ that is a

convex combination of stabilizer states, i.e.

$$\rho = \sum_{|\psi\rangle \text{ stabilizer state}} \lambda_\psi \, |\psi\rangle \langle\psi| \; \in \; SP_n.$$

In this case we can simulate the circuit by sampling from the probability distribution on the stabilizer states induced by λ_ψ and then estimating the circuit's outcome by the Gottesman-Knill theorem [12].

Nevertheless, there is a way to promote the stabilizer formalism to universal quantum computation while profiting from its advantages with respect to fault tolerance. This procedure is called *magic state distillation* and was originally introduced by Bravyi and Kitaev [4]. In the process we *distill* a *magic state* from a distillation scheme that takes auxiliary states form a noisy source as an input. The magic state is then *injected* into the actual circuit and enables to realize a non Clifford gate. Such a gate suffices to promote the circuit to UQC. Essentially is that the states used as auxiliary states lie outside the stabilizer polytope SP_n and have a sufficiently high *robustness* with respect to SP_n (for further information regarding robustness measures see [13][12]). The remaining part of this thesis is devoted to get a better understanding of SP_n.

Character theory for finite abelian groups

In order to analyze the stabilizer polytope we will frequently use the concept of characters (on finite abelian groups), which will be briefly introduced here (the ideas are based on [14, Chapter 2]).

Let $(G, +)$ be a finite abelian group. A *character* is a multiplicative homomorphism $\eta : G \to \{\omega \in \mathbb{C} \,|\, \omega = e^{ix}, x \in \mathbb{R}\}$, i.e., $\eta(g + g') = \eta(g)\eta(g')$ for all $g, g' \in G$. The set of characters itself forms a group, called the *dual group* $\widehat{G}$ of G, where the operation is defined by $(\eta \cdot \eta') \in \widehat{G}$ for $\eta, \hat{\eta} \in \widehat{G}$ and $(\eta \cdot \eta')(g) := \eta(g)\eta'(g)$ for all $g \in G$. Moreover, it holds $G \cong \widehat{G}$ and the set of all characters forms an orthogonal basis of $\mathbb{C}^G$, more precisely $\text{span}\{\eta \in \mathbb{C}^G \,|\, \eta \text{ is a character of } G\} = \mathbb{C}^G$ and

$$\eta^* \eta' = \begin{cases} |G|, & \text{if } \eta = \eta' \\ 0, & \eta \neq \eta'. \end{cases}$$

By the fundamental theorem for finite abelian groups, that is $G \cong \mathbb{Z}/\mathbb{Z}_{n_1} \times \ldots, \times \mathbb{Z}/\mathbb{Z}_{n_r}$ for some $n_1, ..., n_r \in \mathbb{N}$, we can assign a canonical character to each $g \in G$. Every $g = (g_1, ..., g_r) \in G$ defines a unique character $\eta_g \in \widehat{G}$ where $\eta_g(x) = \eta_g(x_1, \ldots x_r) = \prod_{j=1}^r e^{2\pi i g_j x_j / n_j}$.

If G is a group of characteristic 2, i.e., $G = \mathbb{Z}_2 \times \ldots \times \mathbb{Z}_2$, then $\eta_g \in \{-1, 1\}^G$ for all $g \in G$ and $\eta_g(xy) = \eta_g(x)\eta_g(y) \in \{-1, 1\}$.

Isotropic subspaces of $\mathbb{F}_2^{2n}$

Essential will be orthogonality relations in the symplectic vector space $\mathbb{F}_2^{2n}$. Recall that the underlying symplectic inner product is

$$\begin{aligned} \cdot : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} &\to \mathbb{F}_2 \\ (h_1, h_2) &\mapsto h_1 \cdot h_2 := h_1^T \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} h_2 \pmod 2, \end{aligned}$$

where h_1^T denotes the usual transpose. For a set $H \subset \mathbb{F}_2^{2n}$ we define its *orthogonal complement* $H^\perp = \{h' \in \mathbb{F}_2^{2n} \,|\, h' \cdot h = 0 \text{ for all } h \in H\}$. Note that if $H = \text{span}\{h_1, \dots h_k\}$ then $H^\perp = \{h' \in \mathbb{F}_2^{2n} \,|\, h' \cdot h_i = 0,\, i = 1, \dots k\}$ is the kernel of a homogeneous system of linear equalities and therewith a subspace. Moreover, if $\dim H = k$, then $\dim H^\perp = 2n - k$. A subspace H is called *isotropic* if $H \subset H^\perp$.

If we want to count the vertices of the stabilizer polytope, we can do this by counting two quantities:

(1) The number of isotropic subspaces in $\mathbb{F}_2^{2n}$ of dimension n.

(2) The number of abelian subgroups $S \subset \pm P_n \setminus \{-I\}$ such that $r(S) = H$ for a fixed isotropic subspace H.

Here, we will count the first quantity, the second is related to characters on the isotropic subspaces, as we will see in the subsequent chapters.

As H is a subspace of $H^\perp$ (or additively a subgroup) we can define the quotient vector space $H^\perp/H$. We will shortly discuss some basic properties of the quotient. Therefore, we will use the notion of a *coset*, that is for $h' \in \mathbb{F}_2^{2n}$ and a subspace $H \subset \mathbb{F}_2^{2n}$ we define the coset $h' + H := \{h' + h \,|\, h \in H\}$.

If $h_1, ..., h_k, h_{k+1}, ..., h_{2n-k}$ is a basis for $H^\perp$, where $\text{span}\{h_1, ..., h_k\} = H$ and $\text{span}\{h_{k+1}, ..., h_{2n-k}\} = H'$ (if $H = H^\perp$, we set $H' = \{0\}$) then $H^\perp$ can be partitioned into cosets, that is $H^\perp = \dot\cup_{h \in H'}(h + H)$. Thus, $H^\perp/H = \text{span}\{h_{k+1} + H, ..., h_{2n-k} + H\}$ and $H^\perp/H$ has dimension $2n - 2k$. The symplectic inner product on $H/H^\perp$ is naturally inherited from $\mathbb{F}_2^{2n}$, that is $(h+H) \cdot (h'+H) := h \cdot h'$ for $h, h' \in \mathbb{F}_2^{2n}$. This is indeed well-defined because it is independent from the representative of $h + H$ which we can see as follows: for $h_1, h_2 \in H$ it holds $(h + h_1) \cdot (h' + h_2) = h \cdot h'$ since all other inner products cancel if we expand the expression.

As mentioned, to count the number of stabilizer states, we have to count isotropic subspaces.

Proposition 2.2.7. *[15] For $0 \leq m \leq n$ the number of m-dimensional isotropic subspaces of the symplectic vector space $\mathbb{F}_2^{2n}$ is*

$$\prod_{i=0}^{m-1} \frac{2^{2n-i} - 2^i}{2^m - 2^{i-1}}$$

and $H = H^\perp$ is equivalent to H being an n-dimensional isotropic subspace.

Proof. Fix an arbitrary element $h_1 \in \mathbb{F}_2^{2n}$, $h_1 \neq 0$. The set $\{h_1\}^\perp = \{h \in \mathbb{F}_2^{2n} \,|\, h_1 \cdot h = 0\}$ is a $(2n-1)$-dimensional vector space, so we can choose h_2 from $\{h_1\}^\perp$ with the restriction that $h_2 \notin \text{span}\{h_1\} = \{h_1, 0\}$ which leaves $2^{2n-1} - 2$ choices. If we extent the argument to the $i-$th step, we have to choose h_{i+1} from the set $H_i^\perp \setminus \text{span}\{h_1, \ldots, h_i\}$ where $H_i^\perp = \{h_1, ..., h_i\}^\perp$ is a $(2n-i)$-dimensional vector space, thus $|H_i^\perp \setminus \text{span}\{h_1, \ldots, h_i\}| = 2^{2n-i} - 2^i$. In total, we have

$$\prod_{i=0}^{m-1} (2^{2n-i} - 2^i)$$

choices. However, we over-counted because we did not take into account that several bases can span the same space. Therefore, we have to divide by the number of possible bases which can be calculated in the same manner: Let H be an m-dimensional subspace. For the basis' first element h_1 there are $2^m - 1$ possibilities ($h_1 \neq 0$). For the $i-$th element there are $2^m - 2^{i-1}$ choices, hence we have $\prod_{i=0}^{m-1}(2^m - 2^i)$ choices. Division yields

$$\prod_{i=0}^{m-1} \frac{2^{2n-i} - 2^i}{2^m - 2^i}.$$

The fact that $H = H^\perp$ iff H is an n-dimensional isotropic subspace follows immediately from the above construction. □

Apart form self-orthogonal subspaces we are also interested in sets of mutually non-orthogonal elements, that is $h_1, \ldots, h_\ell \in \mathbb{F}_2^{2n}$ such that $h_i \cdot h_j = 1$ for all $i \neq j$, $i, j \in \{1, ..., \ell\}$.

Proposition 2.2.8. *Suppose that $h_1, ..., h_\ell \in \mathbb{F}_2^{2n}$ are linearly independent and that for any $i \in \{1, ..., \ell\}$ there is $j \in \{1, ..., \ell\}$ such that $h_i \cdot h_j = 1$. Then there is a basis $h'_1, ..., h'_\ell$ of $\text{span}\{h_1, ..., h_\ell\}$ such that $h'_i \cdot h'_j = 1$ for all $i \neq j$, $i, j \in \{1, ..., \ell\}$.*

As the proof is of algorithmic nature we introduce the idea with an example. Let $x_1, x_2, z_1, z_2 \in \mathbb{F}_2^4$. Clearly, they are a system of linear independent vectors (they just represent the 4 standard basis vectors in $\mathbb{F}_2^4$) and they satisfy the assumption of the proposition. Now, x_1 is non-orthogonal to z_1 (since X_1 and Z_1 anticommute) but orthogonal to x_2, z_2 and by replacing x_2, z_2 by $z_1 + x_2 = z_1 x_2$ and $z_1 + z_2 = z_1 z_2$ we get a system x_1, z_1, $z_1 x_2$, $z_1 z_2$ that spans the same space and where every element is non-orthogonal to x_1 (except for x_1 itself). The element z_1 is non-orthogonal to x_1 and orthogonal to $z_1 x_2$, $z_1 z_2$, replacing them by $x_1 + z_1 x_2 = y_1 x_2$ and $x_1 + z_1 z_2 = y_1 z_2$ gives a new basis x_1, z_1, $y_1 x_2$, $y_1 z_2$. In the same fashion we can continue with the third element of the new basis but here we are already done since all four elements are mutually non-orthogonal. The proof simply generalizes this idea.

Proof. We set $I_1 = \{h_i \,|\, h_1 \cdot h_i = 0,\, i \in \{2, ..., \ell\}, \}$. Due to the assumptions it holds $|I_1| < \ell$, so assume that $h_2 \notin I_1$. Replacing $h_i \in I_1$ by $h'_i = h_2 + h_i$ and setting $h'_i = h_i$ for all $i \notin I_1$ we get a linearly independent set $h'_1, ..., h'_\ell \in \text{span}\{h_1, ..., h_\ell\}$ that are all non-orthogonal to h'_1.

In the same way we define $I_2 = \{h_i' \mid h_2' \cdot h_i' = 0,\ i \in \{3, ..., \ell\}\}$ and by replacing all elements $h_i' \in I_2$ by $h_i'' = h_1 + h_i'$ and setting $h_i'' = h_i'$ for all $h_i' \notin I_2$ we get a linearly independent set $h_1'', ..., h_\ell'' \in \text{span}\{h_1, ..., h_\ell\}$ that are all non-orthogonal to h_1'' and h_2''.

Continuing in the same fashion and defining $I_3, ..., I_\ell$ as I_1, I_2 before we will eventually end up with some $k \leq \ell$ such that $I_k = I_{k+1} = \cdots I_\ell = \emptyset$ and a system of linearly mutually non-orthogonal elements $h_1^{(k)}, ..., h_\ell^{(k)}$. □

Lemma 2.2.9. *Let H be an isotropic subspace of dimension k and let $m = 2(n-k) = \dim(H^\perp/H)$. Then, there exist $h_1, ..., h_m \in H^\perp$ with $h_i \cdot h_j = 1$ for all $i \neq j$ and*

$$H^\perp/H = \text{span}\{h_1 + H, ..., h_m + H\}.$$

Additionally, the maximal length of a chain mutually non-orthogonal in elements in $H^\perp$ is $m+1$.

Proof. Since $\dim(H^\perp/H) = 2(n-k)$, there are linearly independent $h_1, ..., h_m \in H^\perp$ such that $H^\perp/H = \text{span}\{h_1 + H, ..., h_m + H\}$. Note that for every $h \in H^\perp \setminus H$ there is $h' \in H^\perp \setminus H$ such that $h \cdot h' = 1$, otherwise $H^\perp \subset (\text{span}\{H \cup \{h\}\})^\perp$ but $\dim H^\perp = 2n - k > 2n - k - 1 = \dim(\text{span}\{H \cup \{h\}\})^\perp)$, a contradiction. Hence for every $i = 1, ..., \ell$ there exists $j \in \{1, ..., \ell\}$ such that $h_i \cdot h_j = 1$. Using that $h_i + H \cdot h_j + H = h_i \cdot h_j$ for all $i, j \in \{1, ..., m\}$ we can apply Proposition 2.2.8 and get a basis $h_1' + H, ..., h_m' + H$ for $H^\perp/H$ where $h_i' \cdot h_j' = 1$ for all $i \neq j$.

It remains to show that the maximal length of a chain of non-orthogonal elements is $m+1$. Therefore, we show that if $h_1, ..., h_k$ are mutually non-orthogonal then $h_1, ..., h_k$ are linearly independent or $k = m+1$ is odd and $h_i = \sum_{j \in \{1,...,k\} \setminus \{i\}} h_j$ for all $i = 1, ..., k$. Assume that $h_1 \in \text{span}\{h_2, ..., h_k\}$, that is $h_1 = \sum_{i \in I} h_i$ where $I \subset \{2, \ldots, k\}$. We distinguish two cases:

1. $|I|$ odd:
   Let $j \in I$. Then $h_j \cdot h_1 = \sum_{i \in I} h_j \cdot h_i = |I| - 1 \pmod 2 = 0$. Hence, any linear combination of an odd number of elements in $h_1, ..., h_k$ is orthogonal to the components of the linear combination.

2. $|I|$ even:
   If $|I| < k-1$, there is $j \in \{2, ..., k\} \setminus I$ and $h_j \cdot h_1 = (\sum_{i \in I} h_j \cdot h_i) \pmod 2 = |I| \pmod 2 = 0$.

   If $|I| = k-1$ then k is odd and for all $i = 2, ..., k$, it holds $h_1 \cdot h_i = (\sum_{j=2}^{k-1} h_j \cdot h_i) \pmod 2 = (|I| - 1) \pmod 2 = 1$. Since $h_1 = \sum_{2=1}^{k} h_i$, rearranging yields $h_i = \sum_{j \in \{1,...,k\} \setminus \{i\}} h_j$ for all $i = 1, ..., k$.

Observing that the maximal number of linearly independent elements in $H^\perp/H$ is m we can deduce that there are at most $m+1$ mutually non-orthogonal elements in $H^\perp$. □

An immediate consequence is that the maximal length of mutually non-orthogonal elements in $\mathbb{F}_2^{2n}$ is $2n+1$ which we get if we apply the lemma to the isotropic subspace $H = \{0\}$ (which has dimension 0 and $H^\perp = \mathbb{F}_2^{2n}$).

Another substructure, which will appear oftentimes, are sets that are *closed under addition of orthogonal elements* (CAO for short). A subset $K \subset \mathbb{F}_2^{2n}$ is CAO if $h_1, h_2 \in K$ and $h_1 \cdot h_2 = 0$ then $h_1 + h_2 \in K$. These sets have the following property:

Proposition 2.2.10. *Let $K \subset \mathbb{F}_2^{2n}$ be CAO and $H \subset K$ with $\dim H = k$ where k is the maximal dimension of isotropic subspaces contained in K.*

(i) If $H' \subset \mathbb{F}_2^{2n}$ is an isotropic subspace with $\dim H = s \leq k$, then $H \cap (H')^\perp \subset K$ is an isotropic subspace with $\dim(H \cap (H')^\perp) = k - (s - \dim(H \cap H'))$.

(ii) If $H_1 \subset \mathbb{F}_2^{2n}$ is an isotropic subspace, then there is an isotropic subspace $H_2 \subset K$ with $\dim H_2 = k$ such that $H_1 \subseteq H_2$. In other words, all inclusion maximal isotropic subspaces in K have the same dimension.

Proof. (i) We set $\tilde{H} = H \cap H'$ and $\dim \tilde{H} = r$. Moreover, let $H = \operatorname{span}\{\tilde{H}, h_1, ..., h_p\}$, where $p + r = k$ and $H' = \operatorname{span}\{\tilde{H}, h'_1, ..., h'_q\}$ with $\dim H' = r + q = s \leq k$ and $h'_1, ..., h'_q \notin H$. Since H has maximal dimension among all isotropic subspaces contained in K, it must hold $h'_1, ..., h'_q \notin H^\perp$ (otherwise $\operatorname{span}\{h'_i, H\}$ would be an isotropic subspace of dimension $k + 1$ in K since K is CAO). We start with considering h'_1 and assume without loss of generality that $h'_1 \cdot h_1 = 1$. If $h'_1 \cdot h_i = 1$ for $2 \leq i \leq p$, we argue as in the proof of the last lemma and replace h_i by $h_1 + h_i$ to get $h'_1 \cdot (h_1 + h_i) = 0$, so we may assume that $H_1 := \{h'_1\}^\perp \cap H = \operatorname{span}\{\tilde{H}, h_2, ..., h_p\}$ is a $(k-1)$-dimensional isotropic subspace contained in K.

We continue in the same fashion for $h'_2, ..., h'_q$ by inductively defining $H_i = \{h'_i\}^\perp \cap H_{i-1} = \{h'_1, ..., h'_i\}^\perp \cap H$ for $i = 2, ..., q$. This yields a descending chain with $H_1 \supset H_2 \supset \cdots \supset H_q = (H')^\perp \cap H$ such that $\dim H_i \geq \dim H_{i-1} - 1$ and

$$\dim((H')^\perp \cap H) = \dim(H_q) \geq k - q = k - (s - r) = k - (s - \dim(H \cap H')).$$

For the inequality $\dim((H')^\perp \cap H) \leq k - (s - \dim(H \cap H'))$ we assume the contrary, that is $\dim H_q > k - q$. We consider the isotropic subspace $\operatorname{span}\{H_q, h'_1, ..., h'_q\} \subset K$ (it is indeed contained in K since K is CAO) and claim that it has dimension $\dim H_q + q$. Therefore, we observe that $h'_1, ..., h'_q$ are linearly independent and that $H_q \cap \operatorname{span}\{h'_1, ..., h'_q\} = \{0\}$ due to the assumptions on $h'_1, ..., h'_q$ and the definition of H_q. Hence, by the dimension formula for subspaces, that is $\dim(\operatorname{span}\{H_q, h'_1, ..., h'_q\}) = \dim H_q + \dim(\operatorname{span}\{h'_1, ..., h'_q\}) + \dim(H_q \cap \operatorname{span}\{h'_1, ..., h'_q\}) > (k - q) + q = k$ which contradicts the maximality of the dimension of H.

(ii) If H_1 is an isotropic subspace with $\dim H_1 = s$, the proof of (i) implies that $H_2 :=$

$\operatorname{span}\{H_1, H \cap (H_1)^\perp\}$ contains H_1 and is contained in K and we have

$$\begin{aligned}\dim H_2 &= \dim H_1 + \dim(H \cap (H_1)^\perp) - \dim(\underbrace{H_1 \cap (H \cap (H_1)^\perp)}_{=(H_1 \cap (H_1)^\perp) \cap H = H \cap H_1}) \\ &= s + (k - (s - \dim(H_1 \cap H))) - \dim(H_1 \cap H) \\ &= k.\end{aligned}$$

□

Chapter 3

The Stabilizer Polytope and Contextuality

3.1 The polytope Q_k^f

In this section we will introduce a family of integral polytopes defined as the convex hull of functions $t^* : (\mathbb{F}_2^{2n})^* \to \{0, 1, -1\}$ where $(\mathbb{F}_2^{2n})^* := \mathbb{F}_2^{2n} \setminus \{0\}$. These polytopes can be seen as an integral polytope living in the real Euclidean space $\mathbb{R}^{(\mathbb{F}_2^{2n})^*}$. The exact framework will turn out to be extremely fruitful to analyze the stabilizer polytope SP_n. Under the right assumptions we get a polytope that is just the linear embedding of SP_n into $\mathbb{R}^{(\mathbb{F}_2^{2n})^*}$. We will give a short motivating example why we use this framework.

Instead of considering the actual stabilizer P_S defined in equation (2.5) we can also characterize the stabilizer state by the coefficients if we expand it in the Pauli basis P_n.

For instance, let S be as in Example 2.2.5. We encode the projector P_S by a functional $t : \mathbb{F}_2^4 \to \{0, 1, -1\}$ where $t(r(g)) = \operatorname{Tr}(gP_S)$ for all $g \in P_2$, that is $t(r(I)) = t(x_1x_2) = t(z_1z_2) = 1$, $t(y_1y_2) = t(x_1x_2 + z_1z_2) = -1$ and $t(h) = 0$ for all $h \notin r(S)$.

We generalize this as follows:
Let $f : \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \to \mathbb{C}$ be a function such that $f(h, h) = f(0, h) = f(h, 0) = 1$ and $f(h_1, h_2) \in \{1, -1\}$ if $h_1 \cdot h_2 = 0$. Moreover, let $t : \mathbb{F}_2^{2n} \to \{0, 1 - 1\}$ such that the following two conditions are satisfied:

(A1) $t(h_1) \cdot t(h_2) = 0$ if $h_1 \cdot h_2 = 1$.

(A2) $t(h_1 + h_2) = f(h_1, h_2) \cdot t(h_1) \cdot t(h_2)$ if $h_1 \cdot h_2 = 0$ and $t(h_1), t(h_2) \neq 0$.

As $f(h_1, h_2) \in \{1, -1\}$ for orthogonal elements h_1, h_2 the second condition is equivalent to

$$f(h_1, h_2)t(h_1 + h_2) = t(h_1)t(h_2).$$

Conditions (A1) and (A2) imply that the support of t, defined as

$$\operatorname{supp}\{t\} = \{h \in \mathbb{F}_2^{2n} \mid t(h) \neq 0\},$$

is an isotropic subspace. Since $h \cdot h = 0$ for all $h \in \mathbb{F}_2^{2n}$, it holds

$$t(0) = t(h+h) = f(h,h) \cdot t(h)\, t(h) = t(h) \cdot t(h) = 1.$$

This is indeed what we want since $\operatorname{Tr} P_S = \operatorname{Tr}(P_S \cdot I) = 1$ shall correspond to this value. If we want to fix the cardinality $|\operatorname{supp}\{t\}|$, we impose a third condition for $1 \leq k \leq n$

(A3) $|t| := \sum_{h \in H} |t(h)| = 2^k$.

The third condition fixes the dimension of the isotropic subspace $\operatorname{supp}\{t\}$ to k. If $a : \mathbb{F}_2^{2n} \to \mathbb{R}$ is any function and $M \subset \mathbb{F}_2^{2n}$, we will write $a_{|M} : M \to \mathbb{C}$ for the restriction of a to M.

Definition 3.1.1. (1) We define the set

$$\mathcal{A}_k^f = \{t : \mathbb{F}_2^{2n} \to \{0, 1, -1\} \mid t \text{ satisfies } (A1), (A2), (A3)\}. \tag{3.1}$$

(2) If K is an arbitrary subset of $\mathbb{F}_2^{2n}$, we set

$$\mathcal{A}_k^f(K) = \{t_{|K} : K \to \{0, 1, -1\} \mid t \in \bigcup_{i=1}^{n} \mathcal{A}_i^f,\ \sum_{h \in K} |t(h)| = 2^k\}.$$

We will also write $t \in \mathcal{A}_k^f(K)$ and for $K^* := K \setminus \{0\}$ and $t \in \mathcal{A}_k^f(K)$ we will write t^* instead of $t_{|K^*}$.

We want to examine how two functionals $t, t' \in \mathcal{A}_k^f(K)$ for $K \subset \mathbb{F}_2^{2n}$ are related to each other.

Proposition 3.1.2. *Let $K \subset \mathbb{F}_2^{2n}$ be CAO, $1 \leq k \leq n$, $t \in \mathcal{A}_k^f(K)$ and $H = \operatorname{supp}\{t\} \subset K$.*

(i) It holds

$$\begin{aligned} &\{t' \mid t' \in \mathcal{A}_k^f(K),\ \operatorname{supp}\{t'\} = H\} \\ =&\{\eta t \mid \eta_{|H} : H \to \{1, -1\} \text{ is a character on the additve group } H\}. \end{aligned}$$

Hence, $|\{t' \mid t' \in \mathcal{A}_k^f(K),\ \operatorname{supp}\{t'\} = H\}| = |H|$.

(ii) If $H' \subset K$ is an arbitrary isotropic subspace, then there is a $t' \in \cup_{l=1}^{k} A_l^f(K)$ with $\operatorname{supp}\{t'\} = H \cap H'$ and $t_{|H'} = t'_{|H'}$.

(iii) For every k-dimensional isotropic subspace H it holds

$$\sum_{t \in \mathcal{A}_k^f(K),\, \operatorname{supp}\{t\} = H} t^* = 0.$$

We note that K being CAO ensures that the set $H = \operatorname{supp}\{t\}$ is an isotropic subspace for all $t \in \mathcal{A}_k^f(K)$, $1 \leq k \leq n$.

Proof. (i) Let $t' \in \mathcal{A}_k^f(K)$ and $\mathrm{supp}\{t'\} = H = \mathrm{supp}\{t\}$. Obviously, we can find $\eta : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ with $\eta_{|H} : \mathbb{F}_2^{2n} \to \{1, -1\}$ such that $\eta t = t'$. We have to show that $\eta(h_1 + h_2) = \eta(h_1)g(h_2)$ for all $h_1, h_2 \in H$. By definition, we have

$$\eta(h_1 + h_2) \cdot t(h_1 + h_2) = t'(h_1 + h_2)$$

which, by Condition (A2) becomes

$$\begin{aligned}\eta(h_1 + h_2) \cdot f(h_1, h_2) \cdot t(h_1) \cdot t(h_2) &= f(h_1, h_2) \cdot t'(h_1) \cdot t'(h_2) \\ &= f(h_1, h_2) \cdot \eta(h_1) \cdot t(h_1) \cdot \eta(h_2) \cdot t(h_2)\end{aligned}$$

and dividing by $f(h_1, h_2)t(h_1)t(h_2)$ gives $\eta(h_1 + h_2) = \eta(h_1) \cdot \eta(h_2)$.

Conversely, let $\eta : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ such that $\eta_{|H}$ defines a character on the additive group H. We want to show that $\eta t \in \mathcal{A}_k^f(K)$ and $\mathrm{supp}\{\eta g\} = H$. The Condition (A1) follows directly since $\mathrm{supp}\{\eta g\} = \mathrm{supp}\{g\} \cap \mathrm{supp}\{t\} = H$ is an isotropic subspace. It remains to check that Condition (A2) is satisfied by ηg. Let h_1, h_2 be orthogonal to each other such that $h_1, h_2 \in \mathrm{supp}\{\eta g\} = H$. Then

$$\begin{aligned}(\eta g)(h_1 + h_2) = \eta(h_1 + h_2) \cdot t(h_1 + h_2) &= f(h_1, h_2) \cdot \eta(h_1) \cdot t(h_1) \cdot g(h_2) \cdot t(h_2) \\ &= f(h_1, h_2) \cdot (\eta g)(h_1) \cdot (\eta g)(h_2),\end{aligned}$$

shows that the condition holds. We used that η is a homomorphism on $\mathrm{supp}\{t\}$ in the second equation. Now, $|\{t' \,|\, t' \in \mathcal{A}_k^f(K), \mathrm{supp}\{t'\} = H\}| = |H|$ since the number of characters on the additive group H (which is the cardinality of the dual group $\hat{H}$) coincides with the number of elements in H (due to $H \cong \hat{H}$).

(ii) Let H' be an arbitrary isotropic subspace. Define $t' : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ by

$$t'(h) = \begin{cases} t(h), & \text{if } h \in H \cap H' \\ 0, & \text{otherwise.} \end{cases}$$

Then, conditions (A1) and (A2) hold trivially for t' as $\mathrm{supp}\{t'\} \subset \mathrm{supp}\{t\}$.

(iii) We will show that $\sum_{t \in \mathcal{A}_k^f(K), \mathrm{supp}\{t\} = H} t(h) = 0$ for all $h \in K$. Let $H' \subset H$ be a $(k-1)$-dimensional isotropic subspace in H which does not contain h. We divide H into cosets $H = H' \cup (h + H')$. Now, all elements $t \in \mathcal{A}_k^f(K)$, $\mathrm{supp}\{t\} = H$ are uniquely determined by $t_{|H'} = t'_{|H'}$ for some $t' \in \mathcal{A}_{k-1}^f(K)$, $\mathrm{supp}\{t'\} = H'$ and a fixed value $t(h) \in \{-1, 1\}$. The assignments for elements in the coset $h + h' \in h + H'$ for $h' \in H'$ are determined by $t(h + h') = f(h, h')t(h)t(h') = f(h, h')t(h)t'(h)$.

Hence, we are able to partition the set $\{t \in \mathcal{A}_k^f(K) \,|\, \operatorname{supp}\{t\} = H\}$ into disjoint sets

$$\{t \,|\, t(h) = 1,\, t_{|H'} = t',\, t' \in \mathcal{A}_{k-1}^f(K),\, \operatorname{supp}\{t'\} = H'\},$$
$$\{t \,|\, t(h) = -1,\, t_{|H'} = t',\, t' \in \mathcal{A}_{k-1}^f(K),\, \operatorname{supp}\{t'\} = H'\}$$

of the same cardinality yielding $\sum_{t \in \mathcal{A}_k^f(K),\, \operatorname{supp}\{t\} = H} t(h) = 0$. Since $h \in K$ was chosen arbitrarily in the support of the functions, we have $\sum_{t \in \mathcal{A}_k^f,\, \operatorname{supp}\{t\} = H} t^* = 0$.

□

If we interpret $t, t' \in A_k^f(K)$ as vectors in $\mathbb{R}^K$, we can define their inner product as

$$t^T t' := \sum_{h \in K} t(h) \cdot t'(h).$$

A direct consequence of the proposition is the following:

Corollary 3.1.3. *Let $K \subset \mathbb{F}_2^{2n}$ be CAO and $t, t' \in \mathcal{A}_k^f(K)$ with $H = \operatorname{supp}\{t\} \cap \operatorname{supp}\{t'\}$. Then $t^T t' \in \{0, |H|\}$.*

Proof. Since K is CAO, H is an isotropic subspace we can apply (i) and (ii) of the last proposition to deduce that there is a character $\eta_{|H} : H \to \{-1, 1\}$ such that $\eta_{|H} t_{|H} = t'_{|H}$.

$$\begin{aligned} t^T t' := \sum_{h \in K} t(h)t'(h) &= \sum_{h \in H} t(h)t'(h) \\ &= \sum_{h \in H} \eta(h)t'(h)t'(h) \\ &= \sum_{h \in H} \eta(h) = \begin{cases} |H|, \text{ if } t_{|H} = t'_{|H} \\ 0, \text{ otherwise.} \end{cases} \end{aligned} \tag{3.2}$$

Thus, t and t' are either orthogonal to each other or they are equal on the intersection of their support. □

Based on the set $\mathcal{A}_k^f(K)$ we will now define one of the main objects of this thesis. These are polytopes related to the functions $t \in \mathcal{A}_k^f(K)$.

Definition 3.1.4. For $K \subset \mathbb{F}_2^{2n}$ we define the polytope

$$Q_k^f(K) = \operatorname{conv}\{t^* \,|\, t \in \mathcal{A}_k^f(K)\}$$

and for $K = (\mathbb{F}_2^{2n})^*$

$$Q_k^f := Q_k^f(\mathbb{F}_2^{2n}) = \operatorname{conv}\{t^* \,|\, t \in \mathcal{A}_k^f\}.$$

Example 3.1.5 We consider the case $k = 1$ and arbitrary $K \subset \mathbb{F}_2^{2n}$. Due to the fact $|t| = 2$ for all $t \in \mathcal{A}_1^f$ there is exactly one $h \in (\mathbb{F}_2^{2n})^*$ such that $|t(h)| = 1$ and $t(h') = 0$ for all other $h' \in (\mathbb{F}_2^{2n})^* \setminus \{h\}$. Hence, the functions t^* for $t \in \mathcal{A}_1^f$ coincide with the standard basis vectors of $\mathbb{R}^{(\mathbb{F}_2^{2n})^*}$ with negative or positive sign $\pm e_i \in \mathbb{R}^{(\mathbb{F}_2^{2n})^*}$. Therefore, independently of f, the polytope Q_1^f is the cross polytope, so

$$Q_1^f = \{x : (\mathbb{F}_2^{2n})^* \to \mathbb{R} \mid \sum_{h \in (\mathbb{F}_2^{2n})^*} |x(h)| \leq 1\} \tag{3.3}$$

and for every $K \subset \mathbb{F}_2^{2n}$ we have

$$Q_1^f(K) = \{x : K^* \to \mathbb{R} \mid \sum_{h \in K^*} |x(h)| \leq 1\}.$$

So far, we have left the function f quite variable. Yet, for our purposes we want that it behaves "nicely" in a certain sense. For the case $k = 1$ the last example showed that actual choice of f does not matter (as long as $f(h,h) = f(h,0) = f(0,h) = 1$). Let $H = \operatorname{span}\{h_1, h_2\} = \{h_1, h_2, h_3, 0\}$ be an isotropic subspace. We will derive two necessary conditions for the existence of $t \in \mathcal{A}_2^f$ with $\operatorname{supp}\{t\} = H$. Obviously, we require $f(h_1, h_2) = f(h_2, h_1)$. Moreover, we need that $f(h_1, h_2) = f(h_1, h_1 + h_2) = f(h_1, h_3)$. For suppose not, assume that $f(h_1, h_2) = -f(h_1, h_1 + h_2)$. Then

$$\begin{aligned} t(h_1) \cdot t(h_2) = f(h_1, h_2) \cdot t(h_1 + h_2) &= -f(h_1, h_1 + h_2) \cdot t(h_1 + h_2) \cdot t(h_1) \cdot t(h_1) \\ &= -t(h_1 + h_2 + h_1) \cdot t(h_1) \\ &= -t(h_1) \cdot t(h_2) \end{aligned}$$

forces that $t(h_1)t(h_2) = 0$, so $h_1 \notin \operatorname{supp}\{t\}$ or $h_2 \notin \operatorname{supp}\{t\}$, a contradiction. Thus, we have the following two necessary conditions if we want to find $t \in \mathcal{A}_2^f$ with $\operatorname{supp}\{t\} = H$ for every isotropic subspace H of dimension 2:

1. The function f is symmetric for orthogonal elements, meaning $f(h_1, h_2) = f(h_2, h_1)$ if $h_1 \cdot h_2 = 0$.

2. The function f is constant on $H^* = H \setminus \{0\}$, that is, if $h_1 \cdot h_2 = 0$ and $h_1 + h_2 = h_3$, then $f(h_1, h_2) = f(h_1, h_3) = f(h_2, h_3)$.

From now on we will impose a stronger condition on f, that is for every isotropic subspace H of arbitrary dimension $k \leq n$ there exists $f \in \mathcal{A}_k^f$ such that $\operatorname{supp}\{t\} = H$. For instance, this is satisfied for $f \equiv 1$. Evidently, this also requires that the two above assumptions hold.

The following proposition will establish useful inclusion relations among polytopes $Q_{s_1}^f(K)$ and $Q_{s_2}^f(K)$ for different $1 \leq s_1, s_2 \leq n$ and CAO sets $K \subset \mathbb{F}_2^{2n}$.

Proposition 3.1.6. *Let $1 \leq s_1 \leq s_2 \leq k$ and $K \subset \mathbb{F}_2^{2n}$ be CAO such that the maximal dimension of isotropic subspaces in K is k then $Q_{s_1}^f(K) \subset Q_{s_2}^f(K)$*

Proof. It suffices to show the statement for $s_1 = s_2 - 1$. Let $t \in \mathcal{A}^f_{s_1}(K)$ with $\operatorname{supp}\{t\} = H$ and $\dim H = s_1$. Due to Proposition 2.2.10 (ii) all isotropic subspaces are contained in an isotropic subspace of dimension k, thus there exists $h' \in H^\perp \setminus H \cap K$ such that $H' = \operatorname{span}\{h', H\} = H \dot\cup (h' + H) \subset K$ is an isotropic subspace. We construct $t_1, t_2 \in \mathcal{A}^f_{s_2}(K)$ such that $t = 1/2t_1 + 1/2t_2$ by setting

$$t_1(h) = \begin{cases} t(h), \text{ if } h \in H, \\ 1, \text{ if } h = h' \\ f(h', h'')t(h''), \text{ if } h = h' + h'', \text{ for } h'' \in H \\ 0, \text{ otherwise,} \end{cases}$$

$$t_2(h) = \begin{cases} t(h), \text{ if } h \in H, \\ -1, \text{ if } h = h' \\ -f(h', h'')t(h''), \text{ if } h = h' + h'', \text{ for } h'' \in H \\ 0, \text{ otherwise.} \end{cases}$$

Then $t_1, t_2 \in \mathcal{A}^f_{s_2}(K)$, $\operatorname{supp}\{t_1\} = \operatorname{supp}\{t_2\} = H'$ and $t^* = 1/2t_1^* + 1/2t_2^*$ which implies that $\mathcal{V}(Q^f_{s_1}(K)) \subset Q^f_{s_2}(K)$ and consequently $Q^f_{s_1}(K) \subset Q^f_{s_2}(K)$. □

An immediate consequence of the proposition is that $Q^f_k(K)$ is full-dimensional for every k and every CAO set $K \subset \mathbb{F}_2^{2n}$, $K \neq \emptyset, \{0\}$ since $Q^f_1(K) \subset Q^f_k(K)$ for all $k \geq 1$ and $Q^f_1(K)$ coincides with the full-dimensional cross polytope (Example 3.1.5). Moreover, this inclusion relation will serve useful if we want to describe the dual polytope $(Q^f_k)^\circ$ since the vertices of all Q^f_k for $k \leq s$ will define valid inequalities for $(Q^f_s)^\circ$.

We finish the chapter by stating a remarkable property of the polytope Q^f_k. That is, we will show that $Q^f_k(H)$ is a simplex if H is an isotropic subspace of dimension k. Consider the projection of Q^f_k onto H^*, i.e., $Q^f_k(H)$. Using Proposition 3.1.2 (ii) and 3.1.6 we can rewrite this as

$$Q^f_k(H) := \operatorname{conv}\{t_{|H^*} \,|\, t \in \mathcal{A}^f_k, \operatorname{supp}\{t\} = H\} = \operatorname{conv}\{t^* \,|\, t \in \mathcal{A}^f_k(H)\} \subset \mathbb{R}^{H^*}.$$

Since $|\{t \in \mathcal{A}^f_k\}| = |H|$, the polytope $Q^f_k(H)$ has $|H|$ vertices and it is full-dimensional in a space of dimension $|H|-1$, consequently a simplex. By Corollary 3.1.3, all functions $t \in \mathcal{A}^f_k(H)$ are orthogonal to each other, so $(t_1^*)^T t_2^* = (t_1)^T t_2 - t_1(0)t_2(0) = -1$ for all $t_1, t_2 \in \mathcal{A}^f_k(H)$, $t_1 \neq t_2$. We obtain the following facet description:

$$Q^f_k(H) = \{\ell : H^* \to \mathbb{R} \,|\, \ell^T t^* \geq -1 \text{ for } t \in \mathcal{A}^f_k(H), \operatorname{supp}\{t\} = H\},$$

which implies that $Q^f_k(H)$ is self-dual. Since the functionals t^* define the facet normals, we

have

$$Q_k^f(H^*) = \mathrm{conv}\{t^* \,|\, t \in \mathcal{A}_k^f(H),\, \mathrm{supp}\{t\} = H\} = (Q_k^f(H^*))^\circ \subset \mathbb{R}^{H^*}.$$

Lemma 3.1.7. *If $H \subset \mathbb{F}_2^{2n}$ is a k-dimensional isotropic subspace, then $Q_k^f(H)$ is a self-dual reflexive simplex.*

Q_n^f as the embedding of the stabilizer polytope in the real Euclidean space

The goal of this subsection is to build the bridge between the stabilizer polytope SP_n and Q_n^f. We will see that Q_n^f is the linear embedding of the stabilizer polytope SP_n in the space $\mathbb{R}^{(\mathbb{F}_2^{2n})^*}$. Let $\mathcal{H}_n$ be the space of $2^n \times 2^n$ Hermitian matrices. Recall that if we consider $\mathcal{H}_n$ as a 4^n-dimensional vector space over $\mathbb{R}$ the set of Pauli matrices P_n forms an orthogonal basis and $\mathrm{Tr}\,(g^2) = \mathrm{Tr}\,(I) = 2^n$ for all $g \in P_n$. Hence, we can expand an arbitrary Hermitian matrix $A \in \mathbb{C}^{2^n \times 2^n}$ as

$$A = \frac{1}{2^n} \sum_{g \in P_n} \mathrm{Tr}\,(Ag) g$$

with coefficients $\mathrm{Tr}\,(Ag) \in \mathbb{R}$. We associate the function $t_A : \mathbb{F}_2^{2n} \to \mathbb{R}$ with A where $t_A(r(g)) = \mathrm{Tr}\,(Ag)$ for all $g \in P_n$ (which completely determines t_A since $r(P_n) = \mathbb{F}_2^{2n}$). If ρ is a state, the function t_ρ is also known as the *polarization vector* or *characteristic function* of ρ with respect to P_n (see [15] where it is defined for the more general set of *Weyl operators*).

We have the following identity for $A, B \in \mathcal{H}_n$:

$$\begin{aligned}\mathrm{Tr}\,(AB) = \mathrm{Tr}\left(\Big(\frac{1}{2^n}\sum_{g\in P_n}\mathrm{Tr}\,(Ag)g\Big)\cdot\Big(\frac{1}{2^n}\sum_{g\in P_n}\mathrm{Tr}\,(Bg)g\Big)\right) &= \frac{1}{4^n}\sum_{g\in P_n}\mathrm{Tr}\,(Ag)\cdot\mathrm{Tr}\,(Bg)\cdot\mathrm{Tr}\,(g^2)\\ &= \frac{1}{2^n}t_A^T t_B.\end{aligned}$$

We will now show that the functions associated to stabilizer states are exactly the elements in the set $\mathcal{A}_n^f$ if f is chosen as in (2.3). Let

$$\begin{aligned}\phi : \mathcal{H}_n &\to \{x \,|\, x : \mathbb{F}_2^{2n} \to \mathbb{R}\} \\ A &\mapsto t_A\end{aligned} \tag{3.4}$$

and ϕ^* defined as the canonical projection of ϕ onto $(\mathbb{F}_2^{2n})^*$, i.e., $\phi^*(A) = t_A^*$. Note that ϕ and ϕ^* are linear since they coincide component wise the standard trace function.

Lemma 3.1.8. *Let $H \subset \mathbb{F}_2^{2n}$ be an isotropic subspace with $\dim(H) = k \leq n$ and let f be*

defined as in (2.3). There is a bijection

$$\{S \subset \pm P_n \setminus \{-I\} \,|\, S \text{ abelian subgroup, } r(S) = H\} \longleftrightarrow \{t \in \mathcal{A}_k^f \,|\, \mathrm{supp}\{t\} = H\} \longleftrightarrow \{t \,|\, t \in \mathcal{A}_k^f(H)\}.$$

Furthermore, Q_n^f is the image of the stabilizer polytope SP_n under ϕ^*, i.e., $\phi^*(SP_n) = Q_n^f$.

For the proof we recall that the projector onto the common $+1$ eigenspace of an abelian subgroup $S \subset \pm P_n \setminus \{-I\}$ is defined as $P_S = 1/2^k \sum_{g \in S} g$.

Proof. The second part of the bijection is clear and follows from the definitions of $\mathcal{A}_k^f$ and $\mathcal{A}_k^f(H)$. Let $S \subset \pm P_n \setminus \{-I\}$ be an abelian subgroup with $r(S) = H$ and projector P_S. We will show that $t_{P_S} \in \mathcal{A}_k^f$. Therefore, note that for $g \in P_n$

$$t_{P_S}(r(g)) = \mathrm{Tr}\,(P_S \cdot g) = \begin{cases} 1, \text{ if } g \in S \\ -1, \text{ if } -g \in S \\ 0, \text{ otherwise.} \end{cases} \tag{3.5}$$

Hence, $t_{P_S}(r(g)) = \chi(g) \in \{1, -1\}$ for all $g \in S$ and $t(h) = 0$ for all $h \notin r(S)$. So, we obviously have $\mathrm{supp}\{t\} = r(S) = H$, which is an isotropic subspace, and $\sum_{h \in \mathbb{F}_2^{2n}} |t(h)| = 2^k$, thus (A1) and (A3) hold for t_{P_S}. For (A2) let $h_1, h_2 \in \mathrm{supp}\{t_{P_S}\}$ with $r(g_i) = h_i$ for $g_1, g_2 \in S$, $i = 1, 2$. The identity (2.4) yields

$$\begin{aligned} f(h_1, h_2) \cdot t_{P_S}(h_1) \cdot t_{P_S}(h_2) &= \Big(\underbrace{\chi(g_1) \cdot \chi(g_2) \cdot \chi(g_1 g_2)}_{= f(h_1, h_2)} \Big) \cdot \chi(g_1) \cdot \chi(g_2) \\ &= \chi(g_1 g_2) \\ &= t_{P_S}(r(g_1 g_2)) \\ &= t_{P_S}(r(g_1) + r(g_2)) \\ &= t_{P_S}(h_1 + h_2), \end{aligned}$$

which shows the desired property and $t_{P_S} \in \mathcal{A}_f^k$ (respectively, $(t_{P_S})_{|H} \in \mathcal{A}_k^f(H)$).

Conversely, assume that $t \in \mathcal{A}_k^f$. We construct the associated abelian subgroup S as follows: We define

$$S = \{g \in \pm P_n \,|\, r(g) \in \mathrm{supp}\{t\},\, \chi(g) = t(r(g))\}. \tag{3.6}$$

Clearly, all elements in S commute because $\mathrm{supp}\{t\}$ is an isotropic subspace. We have to check that S is closed under multiplication. This is satisfied if it holds $\chi(g_1 g_2) = t(r(g_1 g_2))$ for all $g_1, g_2 \in S$. Due to identity (2.4) and Condition (A2) for t we obtain

$$\chi(g_1 g_2) = \chi(g_1) \cdot \chi(g_2) \cdot f(r(g_1), r(g_2)) = t(r(g_1)) \cdot t(r(g_2)) \cdot f(r(g_1), r(g_2)) = t(r(g_1 g_2)),$$

which proves that S is closed under multiplication and therewith an abelian subgroup.

To prove that $\psi(SP_n) = Q_n^f$ it suffices to note that if P_S is a rank one projector (i.e., a projector onto a stabilizer state) then $\phi(P_S) = t_{P_S} \in \mathcal{A}_n^f$. Using the above constructed bijection it follows that $\phi(\mathcal{V}(SP_n)) = \mathcal{A}_n^f$, so $\phi^*(\mathcal{V}(SP_n)) = \mathcal{V}(Q_n^f)$ and due to the linearity of ϕ^*, eventually $\phi(SP_n) = Q_n^f$. □

The lemma shows that we can basically consider SP_n and Q_n^f as the same objects - just embedded in another space. We have the following corollary:

Corollary 3.1.9. *Let $S, S' \subset \pm P_n \setminus \{-I\}$ be abelian subgroups with $r(S) = r(S') = H$. Then there is a character $\eta : H \to \{1, -1\}$ such that*

$$P_{S'} = \frac{1}{|S|} \sum_{g \in S} \eta(r(g)) \cdot g.$$

Proof. Let $\phi(P_S) = t_{P_S}$ and $\phi(P_{S'}) = t_{P_{S'}} \in \mathcal{A}_n^f$. Due to Proposition 3.1.2 (i) there is a character $\eta : \mathbb{F}_2^{2n} \to \{1, -1\}$ such that η_H is a character on H and $\eta t_{P_S} = t_{P_{S'}}$. Thus, we have

$$\begin{aligned} P_{S'} = \frac{1}{|S'|} \sum_{g \in P_n} \mathrm{Tr}\left(P_{S'} g\right) \cdot g &= \sum_{g \in r^{-1}(H) \cap P_n} t_{P_{S'}}(r(g)) \cdot g \\ &= \frac{1}{|S'|} \sum_{g \in r^{-1}(H) \cap P_n} \Big(\eta(r(g)) \cdot t_{P_S}(r(g))\Big) \cdot g \\ &= \frac{1}{|S|} \sum_{g \in S} \eta(r(g)) \cdot g \end{aligned}$$

□

Finally, we have all the tools to determine the dimension of the common $+1$ eigenspace of elements in an abelian subgroup $S \subset \pm P_n \setminus \{-I\}$. This will also provide the missing part for the proof of Theorem 2.2.4 in Section 2.2.

Lemma 3.1.10. *Let $S = \langle g_1, ..., g_{n-k} \rangle \subset \pm P_n \setminus \{-I\}$ be an abelian subgroup such that $r(g_1), ..., r(g_{n-k}) \in \mathbb{F}_2^{2n}$ are linearly independent and let $V_S = \{|\psi\rangle \mid g\,|\psi\rangle = |\psi\rangle \text{ for all } g \in S\}$ the subspace invariant under actions form S. Then $\dim(V_S) = 2^k$.*

Proof. Let $H = \mathrm{span}\{h_1, ..., h_{n-k}\}$ be an isotropic subspace of dimension $n-k$ and let $S \subset \pm P_n \setminus \{-I\}$ be an abelian subgroup with $r(S) = H$ and projector $P_S = 1/2^{n-k} \sum_{g \in S} g$ onto the code space V_S. We fix $g_1, ..., g_{n-k} \in S$ with $r(g_i) = h_i$. Each character $\eta : H \to \{1, -1\}$ is uniquely determined by its image on the set of generators, i.e., by $\eta(h_i) \in \{1, -1\}$, $i = 1, ..., n-k$. Hence, we can encode each character as η_a, where $a \in \{-1, 1\}^{n-k}$ and

$\eta_a(h_i) = a_i$. Due to Corollary 3.1.9 each projector can be written as

$$P_{S,a} = \prod_{i=1}^{n-k} \left(\frac{I + a_i \cdot g}{2} \right) = \frac{1}{2^{n-k}} \sum_{g \in S} \eta_a(r(g)) g. \tag{3.7}$$

The projectors are orthogonal to each other since for $a \neq a'$ we have

$$P_{S,a} \cdot P_{S,a'} = \prod_{i=1}^{n-k} \left(\frac{(I + a_i \cdot g)(I + a'_i \cdot g)}{4} \right) = \frac{1}{2^{2(n-k)}} \prod_{i=1}^{n-k} \underbrace{(I + a_i \cdot g + a'_i \cdot g + a_i a'_i I)}_{=0, \text{ if } a_i \neq a'_i}$$
$$= 0.$$

We will show that all projectors $P_{S,a}$ have the same dimension as P_S. Therefore, let $H_j = \text{span}\{h_i \,|\, i \in \{1, ..., n-k\} \setminus \{j\}\}$. Then $\dim(H_j) < n$ for all $k \geq 0$ and there is $h \in H_j^\perp$ such that $h_j \cdot h = 1$, implying that there exists $g \in P_n$ with $r(g) = h$ such that $g g_i g^\dagger = g_i$ for $i \neq j$ and $g g_i g^\dagger = -g_i$. If we pick such a g for all j with $a_j = -1$ and define their product as U (which is a unitary), we get $U g_j U^\dagger = g_j$ if $a_j = 1$ and $U g_j U^\dagger = -g_j$ if $a_j = -1$. Consequently,

$$U P_S U^\dagger = P_{S,a},$$

so the rank of the projector $P_{S,a}$ equals the rank of P_S. Now, $\dim(P_{S,a}) = 2^k$ because we have the identity

$$\begin{aligned}
\sum_{a \in \{1,-1\}^{n-k}} P_{S,a} &= \frac{1}{2^{n-k}} \sum_{a \in \{1,-1\}^{n-k}} \sum_{g \in S} \eta_a(r(g)) g \\
&= \frac{1}{2^{n-k}} \sum_{a \in \{1,-1\}^{n-k}} \sum_{g \in S} \eta_a(r(g)) \cdot g \\
&= \frac{1}{2^{n-k}} \sum_{g \in S} \Big(\underbrace{\sum_{a \in \{1,-1\}^{n-k}} 1 \cdot \eta_a(r(g))}_{= \begin{cases} 2^{n-k}, \text{ if } r(g) = r(I) = 0, \\ 0, \text{ otherwise} \end{cases}} \Big) \cdot g \\
&= I.
\end{aligned}$$

Since the projectors are orthogonal to each other and their rank has to sum up to the rank of I, which is 2^n, every projector has rank 2^k and thus the codespace V_S, where P_S projects to, has dimension 2^k. □

Edges of Q_n^f

Using some properties of our symplectic vector space $\mathbb{F}_2^{2n}$ we are also able to characterize the edges of Q_n^f which also determines the edges of SP_n as we have seen in the last subsection.

The results we derive here are separate form the rest of the thesis and will have no further implications.

Along the proofs we will explain why this cannot be easily generalized to arbitrary $k \leq n$. Moreover, we will not consider a projection on some CAO set $K \subset \mathbb{F}_2^{2n}$, however, a careful adaption to this case might be possible. For two sets S_1, S_2 we define the symmetric difference $S_1 \triangle S_2$ as

$$S_1 \triangle S_2 = (S_1 \setminus S_2) \cup (S_2 \setminus S_1).$$

Proposition 3.1.11. *Let $H, H_1, H_2 \subset \mathbb{F}_2^{2n}$ be n-dimensional isotropic subspaces with $|H| = |H_1| = |H_2|$. Then*

$$|(H_1 \triangle H_2) \cap H| \leq |H_1 \setminus H_2| = |H_2 \setminus H_1|$$

and equality holds if and only if $H \in \{H_1, H_2\}$ or $H_1 = H_2$.

Proof. The statement is trivially true if we have equality for $H \in \{H_1, H_2\}$ or $H_1 = H_2$. So we assume that non of these cases is true. Let

$$\begin{aligned} \dim(H \cap H_1 \cap H_2) &= p \\ \dim(H \cap H_1) &= p + q \\ \dim(H \cap H_2) &= p + r \\ \dim(H_1 \cap H_2) &= p + s. \end{aligned}$$

As the dimension of all three subspaces is n we get the following restrictions for p, q, r, s:

$$p + q + r \leq n, \text{ due to } \dim H = n, \tag{3.8}$$
$$p + q + s \leq n, \text{ due to } \dim H_1 = n, \tag{3.9}$$
$$p + r + s \leq n, \text{ due to } \dim H_2 = n. \tag{3.10}$$

The set $(H_1 \triangle H_2) \cap H$ can be rewritten as

$$(H_1 \triangle H_2) \cap H = \Big((H_1 \cap H) \setminus (H_1 \cap H_2 \cap H)\Big) \cup \Big((H_2 \cap H) \setminus (H_1 \cap H_2 \cap H)\Big),$$

implying

$$|(H_1 \triangle H_2) \cap H| = (2^{q+p} - 2^p) + (2^{r+p} - 2^p). \tag{3.11}$$

We consider three cases:

1. $s = 0$:
   Then $H \cap H_1 \cap H_2 = H_1 \cap H_2$. Moreover, $p + q < n$ and $p + r < n$ since $H \notin \{H_1, H_2\}$

and we can compute

$$(2^{q+p} - 2^p) + (2^{r+p} - 2^p) \leq 2^{n-1} + 2^{n-1} - 2^{p+1} \leq 2^n - 2^{p+1} < 2^n - 2^p,$$

where the last expression equals $|H_1 \setminus H_2| = |H_1 \setminus (H_1 \cap H_2)| = |H_1 \setminus (H_1 \cap H_2 \cap H)|$.

2. $s > 1$:
Using inequalities (3.9) and (3.10) we get

$$\begin{aligned}(2^{q+p} - 2^p) + (2^{r+p} - 2^p) \leq 2^{n-s} + 2^{n-s} - 2^{p+1} &= 2^{n-s+1} - 2^{p+1} \\ &= 2^{p+1}(2^{n-s-p} - 1) \\ &< 2^{s+p}(2^{n-s-p} - 1) \\ &= 2^n - 2^{p+s} \\ &= |H_1 \setminus H_2|.\end{aligned}$$

3. $s = 1$:
We claim that $p + q + s < n$ or $p + r + s < n$. Therefore, assume the contrary, i.e., $p + q = p + r = n - s = n - 1$. Then $p + q = p + r = n - 1$ and $p + q + r \leq n$ (inequality (3.8)) imply $q = r \leq 1$. If $q = r = 0$, then $p + s = n$ which is equivalent to $H_1 = H_2$. So, let $q = r = 1$ and $p = n - 2$. Note that we have $\dim(H \cap H_1) = \dim(H \cap H_2) = \dim(H \cap H_3) = n - 1$ and $\dim(H \cap H_1 \cap H_2) = p = n - 2$. We set $H' = H \cap H_1 \cap H_2 = \text{span}\{u_1, ..., u_p\}$ and fix three elements

$$h_1 \in (H \cap H_1) \setminus H_2, \quad h_2 \in (H \cap H_2) \setminus H_1, \quad h_{12} \in (H_1 \cap H_2) \setminus H.$$

Due to their choice it has to hold $H = \text{span}\{H', h_1, h_2\}$, $H_1 = \text{span}\{H', h_1, h_{12}\}$ and $H_2 = \text{span}\{H', h_2, h_{12}\}$, thus $h_1 \cdot h_2 = h_1 \cdot h_{12} = h_2 \cdot h_{12} = 0$. However, since the dimension of H_1, H_2 and H is n we have $H = H^\perp$ and $H_i = H_i^\perp, H_i = H^\perp$ for $i = 1, 2$ (see the proof of Proposition 2.2.7 for an explanation), but $h_1 \notin H_2 = H_2^\perp$ which contradicts $h_1 \cdot h_2 = h_1 \cdot h_{12} = 0$ and $h_1 \cdot u_i = 0$ for $i = 1, ..., p$.

Hence, we may assume that $p + q + s < n$ and we get the following inequality:

$$\begin{aligned}(2^{q+p} - 2^p) + (2^{r+p} - 2^p) < 2^{n-s} + 2^{n-s} - 2^{p+1} &= 2^{p+1}(2^{n-s-p} - 1) \\ &= 2^{s+p}(2^{n-s-p} - 1) \\ &= 2^n - 2^{s+p} \\ &= |H_1 \setminus H_2|.\end{aligned}$$

To conclude, we have $|(H_1 \triangle H_2) \cap H| < |H_1 \setminus H_2|$ if $H \notin \{H_1, H_2\}$ or $H_1 = H_2$. □

Remark 3.1.12 Note that we only required the property that the subspaces are isotropic

and have dimension n in the third case. Yet, this property cannot be translated to (general) subspaces of smaller dimension or which are not isotropic.

The lemma enables us to determine the edges of Q_n^f:

Lemma 3.1.13. *Let $t_1^*, t_2^* \in \mathcal{V}(Q_n^f)$ be vertices and $t_1, t_2 \in \mathcal{A}_k^f$ the associated functionals. The line segment $[t_1^*, t_2^*]$ is an edge of Q_n^f if and only if* $\operatorname{supp}\{t_1\} \neq \operatorname{supp}\{t_2\}$.

Proof. Let $H_i = \operatorname{supp}\{t_i\}$ for $i = 1, 2$ and suppose that $H_1 \neq H_2$. We define the functional $t_{H_1 \triangle H_2} : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ by

$$t_{H_1 \triangle H_2}(h) = \begin{cases} t_1(h), & \text{if } h \in H_1 \setminus H_2 \\ t_2(h), & \text{if } h \in H_2 \setminus H_1 \\ 0, & \text{otherwise.} \end{cases}$$

Then

$$t_1^T(t_{H_1 \triangle H_2}) = \sum_{h \in H_1 \setminus H_2} t(h) \cdot t(h) = |H_1 \setminus H_2| = |H_2 \setminus H_1| = t_2^T(t_{H_1 \triangle H_2}).$$

Thus, the inner product of $t_{H_1 \triangle H_2}$ with points on the line $[t_1, t_2]$ is constant (and equivalently the inner product of $t^*_{H_1 \triangle H_2}$ with points on the line $[t_1^*, t_2^*]$). In order to show that the line defines an edge we have to prove that $(t^*)^T(t^*_{H_1 \triangle H_2}) < |H_1 \setminus H_2|$ for every $t^* \in \mathcal{V}(Q_k^f) \setminus \{t_1, t_2\}$ with $t \in \mathcal{A}_k^f$. Let $H = \operatorname{supp}\{t\}$. We obtain the following inequality:

$$\begin{aligned} t^T(t_{H_1 \triangle H_2}) &= \sum_{h \in (H_1 \triangle H_2) \cap H} t(h) \cdot t_{H_1 \triangle H_2}(h) \\ &= \sum_{h \in (H_1 \setminus H_2) \cap H} t(h) \cdot t_1(h) + \sum_{h \in (H_2 \setminus H_1) \cap H} t(h) \cdot t_2(h) \\ &\leq \sum_{h \in (H_1 \setminus H_2) \cap H} 1 + \sum_{h \in (H_2 \setminus H_1) \cap H} 1 \\ &= |(H_1 \triangle H_2) \cap H| \\ &\leq |H_1 \setminus H_2|, \end{aligned}$$

where we applied Proposition 3.1.11 in the last step. Now, the first inequality is strict if $H \in \{H_1, H_2\}$ but $t \notin \{t_1, t_2\}$ and the second is strict if $\operatorname{supp}\{t\} \notin \{H_1, H_2\}$, implying that it is always strict whenever $t \in \mathcal{A}_n^f \setminus \{t_1, t_2\}$, so $[t_1^*, t_2^*]$ is an edge of Q_n^f.

Conversely, assume that $H_1 = H_2$. We partition $H_1 = H^{(\neq)} \dot\cup H^{(=)}$ where

$$H^{(\neq)} := \{h \in H_1 \,|\, t_1(h) = -t_2(h)\}, \quad H^{(=)} := H_1 \setminus H^{(\neq)} = \{h \in H_1 \,|\, t_1(h) = t_2(h)\}.$$

Observe that it holds $|H^{(\neq)}| = |H^{(=)}|$ since $t_1^T t_2 = 0$ (due to Corollary 3.1.3). The inner

product of points on the line $[t_1, t_2]$ with a functional $a : \mathbb{F}_2^{2n} \to \mathbb{R}$ has to be constant, that is

$$\begin{aligned} 0 = a^T(t_1 - t_2) &= \sum_{h \in H^{(=)}} a(h) \cdot (t_1(h) - t_2(h)) + \sum_{h \in H^{(\neq)}} a(h) \cdot (t_1(h) - t_2(h)) \\ &= 2 \sum_{h \in H^{(\neq)}} a(h) \cdot t_1(h) \\ &= -2 \sum_{h \in H^{(\neq)}} a(h) \cdot t_2(h), \end{aligned}$$

which forces that $a^T t_1 = a^T t_2 = \sum_{h \in H^{(=)}} a(h) \cdot t(h)$. In order to show that $[t_1^*, t_2^*]$ is not an edge we have to show the existence of $t \in \mathcal{A}_n^f$ such that $a^T t \geq a^T t_1$. Due to the conditions (A1) and (A2) holding for t_1 and t_2 we can deduce that $H^{(=)}$ is an isotropic subspace contained in H with $\dim(H^{(=)}) = \dim(H) - 1 = n - 1$ and $\dim(H^{(=)})^\perp = 2n - (n-1) = n + 1$. Hence, the dimension of the quotient $(H^{(=)})^\perp / H^{(=)}$ is 2, implying that $(H^{(=)})^\perp / (H^{(=)})$ contains a non-trivial element $h + H^{(=)} \neq H^{(=)}$. This guarantees the existence of $t \in \mathcal{A}_n^f$ such that $\text{supp}\{t\} = \text{span}\{H, h\}$ and $t_{|H^{(=)}} = (t_1)_{|H^{(=)}}$ where $t \notin \{t_1, t_2\}$. Since $a^T t = \sum_{h \in H^{(=)}} a(h) t(h) = \sum_{h \in H^{(=)}} a(h) t_1(h) = a^T t_1$, the line segment between t_1^* and t_2^* cannot form an edge of Q_k^f. □

3.2 Characterizing integral points in $(Q_k^f)^\circ$

This whole section will be devoted to determine the integral points in the polar dual of $Q_k^f(K)$ for $K \subset \mathbb{F}_2^{2n}$ being CAO. The property CAO will be once again crucial. Recall that if $Q = \text{conv}\{v_1, ..., v_N\} \subset \mathbb{R}^d$ is a polytope, then $Q^\circ = \{x \in \mathbb{R}^d \,|\, v_i^T x \geq -1,\ i = 1, ..., N\}$. Determining integral points means that we want to characterize functionals $t^\circ : K \to \mathbb{Z}$ with $t^\circ(0) = 1$ that satisfy

$$(t^\circ)^T t = t^\circ(0) t(0) + \sum_{h \in (\mathbb{F}_2^{2n})^*} t^\circ(h) t(h) = 1 + (t^{\circ,*})^T (t^*) \geq 0 \tag{3.12}$$

for all $t \in \mathcal{A}_k^f(K)$. The definition of $Q_k^f(K)$ ensures that for every t° satisfying (3.12) it holds $t^{\circ,*} := t_{|K^*} \in (Q_k^f)^\circ$. Instead of considering elements in the dual polytope we will focus on functionals of the form $x : K \to \mathbb{R}$ with $0 \in K$ and $x(0) = 1$. The condition $(x_{|(\mathbb{F}_2^{2n})^*})^T t^* \geq -1$ translates to $x^T t \geq 0$ for $t \in \mathcal{A}_k^f(K)$. Proposition 3.1.6 ($Q_{s_1}^f(K) \subset Q_{s_2}^f(K)$ for $s_1 \geq s_2 \geq k$ and K being CAO such that the largest isotropic subspace in K has dimension k) yields the implication that if the above equation (3.12) holds for all $t \in \mathcal{A}_f^k(K)$ it holds likewise for all $t \in \mathcal{A}_i^f(K)$ for $i = 1, ..., k$..

Therefore, we can restrict to functions $t^\circ : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ since $(t^\circ)^T t \geq 0$ for all $t \in \mathcal{A}_1^f(K)$ is equivalent to $1 \pm t^\circ(h) \geq 0$ for all $h \in (\mathbb{F}_2^{2n})^*$ implying $-1 \leq t^\circ(h) \leq 1$. As we will see, the set $\text{supp}\{t^\circ\}$ for $t^{\circ,*} \in (Q_k^f(K))^\circ$ has a particular interesting structure for certain functions f, including f defined as in (2.3), which allows us to deduce statements about the stabilizer polytope.

Definition 3.2.1. We define

$$\mathcal{B}^f := \mathcal{B}^f(\mathbb{F}_2^{2n}) = \{t^\circ : \mathbb{F}_2^{2n} \to \{0,1,-1\} \mid t^\circ \text{ satisfies (A2)}\}$$

and for $K \subset \mathbb{F}_2^{2n}$

$$\mathcal{B}^f(K) := \{t^\circ_{|K} : K^* \to \{0,1,-1\} \mid t^\circ \in \mathcal{B}^f\}.$$

As before, we will also write $t^\circ \in \mathcal{B}^f(K)$ and $t^{\circ,*}$ for $t^\circ_{|K^*}$.

Theorem 3.2.2. *Let $k \geq 2$, $K \subset \mathbb{F}_2^{2n}$ such that K is CAO and let $t^\circ : K \to \{0,1,-1\}$ with $t^\circ(0) = 1$. Then $t^{\circ,*} \in (Q_k^f(K))^\circ$ if and only if $t^\circ \in \mathcal{B}^f(K)$.*

An immediate consequence is that $Q_k^f(K) \subset (Q_k^f(K))^\circ$ if $K \subset \mathbb{F}_2^{2n}$ is CAO. because of $\cup_{i=1}^n \mathcal{A}_i^f(K) \subset \mathcal{B}^f$.

If K is CAO, then $t^\circ \in \mathcal{B}^f(K)$ is equivalent to t° being an integral point in $(Q_k^f(K))^\circ$. In contrast to $\mathcal{A}_k^f$ we choose $\mathcal{B}^f$ independent of the 1-norm of the functions, i.e., of k. Condition (A2) forces that $\operatorname{supp}\{t^\circ\}$ is CAO because it implies that $|t^\circ(h+h')| = |t^\circ(h)||t^\circ(h')|$ for $h \cdot h' = 0$ with $h, h' \in \operatorname{supp}\{t^\circ\}$.

Proof. Let $t^\circ \in \mathcal{B}^f(K)$ and $t \in \mathcal{A}_k^f(K)$. Since $\operatorname{supp}\{t^\circ\}$ is CAO, the intersection $H := \operatorname{supp}\{t\} \cap \operatorname{supp}\{t^\circ\}$ is an isotropic subspace. Hence, we can apply Proposition 3.1.2 (i), (ii) and obtain a character $\eta_{|H} : H \to \{1,-1\}$ such that $t_{|H}\eta_{|H} = t^\circ_{|H}$. Thus,

$$(t^\circ)^T t = \sum_{h\in H} t^\circ(h)t(h) = (t^\circ_{|H})^T t_{|H} = \sum_{h\in H} \eta(h) = \begin{cases} |H|, \text{ if } t^\circ_{|H} = t_{|H}, \\ 0, \text{otherwise.} \end{cases}$$

By equation (3.12), it follows $t^{\circ,*} \in (Q_k^f(K^*))^\circ$.

Conversely, assume that $t^\circ \notin \mathcal{B}^f(K)$, i.e., there are $h_1, h_2 \in K$ with $h_1 \cdot h_2 = 0$, $t^\circ(h_1), t^\circ(h_2) \neq 0$ and $t^\circ(h_1+h_2) \neq f(h_1,h_2)\cdot t^\circ(h_1)\cdot t^\circ(h_2)$. Note that $h_1, h_2 \neq 0$, otherwise (A2) is satisfied due to the restrictions on f (that is, $f(0,0) = f(h,0) = f(0,h) = 1$). Let $t \in \mathcal{A}_2^f(K)$ with $t(h_i) = -t^\circ(h_i)$ for $i = 1,2$ and $t(h_1+h_2) = f(h_1,h_2)t(h_1)t(h_2) \neq f(h_1,h_2)t^\circ(h_1)t^\circ(h_2)$. Since t° is integral, we have

$$\begin{aligned}(t^\circ)^T t &= t^\circ(0)t(0) + t^\circ(h_1)t(h_1) + t^\circ(h_2)t(h_2) + \underbrace{t^\circ(h_1+h_2)t(h_1+h_2)}_{\leq 0} \\ &\leq 1 - 1 - 1 = -1\end{aligned}$$

and consequently $(t^{\circ,*})^T t^* \leq -2$, so $t^{\circ,*} \notin (Q_k^f(K^*))^\circ$. □

The above theorem does not hold for $k = 1$. In this case $Q_1^f(K)$ is the cross polytope for all $K \subset \mathbb{F}_2^{2n}$, $K \neq \emptyset, \{0\}$ and $((Q_1^f)(K))^\circ = [-1,1]^{K^*}$ is the hypercube and all functionals

$t^* : K \to \{0, 1, -1\}$ lie in the dual polytope. However, it implies that the set of integral points is stable for all $k \geq 2$. This follows because constraint (A2) just affects isotropic subspaces of dimension 2. Since we have the inclusion $(Q_s^f(K))^\circ \subset (Q_k^f(K))^\circ$ for all $1 \leq k \leq s \leq n$ and $K \subset \mathbb{F}_2^{2n}$ being CAO, the polytope $Q_k^f(K)$ cannot be reflexive (i.e., $(Q_k^f)^\circ$ is not integral) for all $2 \leq k < n$.

We impose two extra conditions on the function f because they are also valid for the choice of f defined in (2.3), allowing us to deduce interesting properties of the stabilizer polytope. Recall that we always assume that for every k-dimensional isotropic subspace H there is $t \in \mathcal{A}_k^f$ such that $\mathrm{supp}\{t\} = H$. Moreover, we have seen that this forces f to be *symmetric for orthogonal elements*, i.e., $f(h_1, h_2) = f(h_2, h_1)$ for all $h_1, h_2 \in \mathbb{F}_2^{2n}$ with $h_1 \cdot h_2 = 0$, and f to be constant on sets h_1, h_2, h_3 where $h_1 \cdot h_2 = 0$ and $h_1 + h_2 = h_3$, i.e., $f(h_1, h_2) = f(h_1, h_3) = f(h_2, h_3)$. From now on we will additionally assume that f satisfies the following two conditions:

3. f is *antisymmetric for non-orthogonal elements*, i.e., $f(h_1, h_2) = -f(h_2, h_1)$ if $h_1 \cdot h_2 = 1$.

4. f is *bilinear*, i.e., $f(h_1 + h, h_2) = f(h_1, h_2)f(h, h_2)$ and $f(h_1, h + h_2) = f(h_1, h)f(h_1, h_2)$ for all $h_1, h_2, h \in \mathbb{F}_2^{2n}$.

Due to Proposition 2.2.1 they both hold for f of (2.3).

Our goal is to characterize the set $\mathrm{supp}\{t^\circ\}$ for $t^\circ : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ with $t^{\circ,*} \in (Q_k^f)^\circ$ (which is equivalent to $t^\circ \in \mathcal{B}^f$) by applying the characterization given in Theorem 3.2.2. We will associate an undirected graph with $G = (V, E)$ with the phase space $\mathbb{F}_2^{2n}$ where $V = \mathbb{F}_2^{2n}$ and

$$E = \{\{h_1, h_2\} \in \mathbb{F}_2^{2n} \times \mathbb{F}_2^{2n} \,|\, h_1 \cdot h_2 = 0\}.$$

The graph will be referred to as the *orthogonality graph* (or *commutativity graph*, as orthogonality in the phase space reflects commutativity in the Pauli group). For a subset $W \subseteq \mathbb{F}_2^{2n}$ the *graph induced by* W is defined as $G(W) = (W, E')$ with $E' = \{\{u, v\} \in E \,|\, u, v \in W\}$. Note that not all subgraphs of a graph are induced by a subset $W \subset V$.

We are especially interested in the graph $G(\mathrm{supp}\{a\})$ for $a : \mathbb{F}_2^{2n} \to \mathbb{R}$. For instance, let $t \in \mathcal{A}_k^f$ with $\mathrm{supp}\{t\} = H$. Then $G(H)$ is a clique (i.e., a graph where all vertices are connected by edges) with 2^k vertices. The structure of $G(\mathrm{supp}\{t^{\circ,*}\})$ becomes more evolved for $t^\circ \in \mathcal{B}^f$. There will be particularly one main "forbidden" substructure. We introduce it as follows:

Definition 3.2.3. Let

$$\boxplus = \{h_{ij} \in \mathbb{F}_2^{2n} \,|\, i, j \in \{1, 2, 3\}\} \cup \{0\}$$

such that $\boxplus$ satisfies the following relations for all $i, j \in \{1, 2, 3\}$ (where the index arithmetic is done modulo 3):

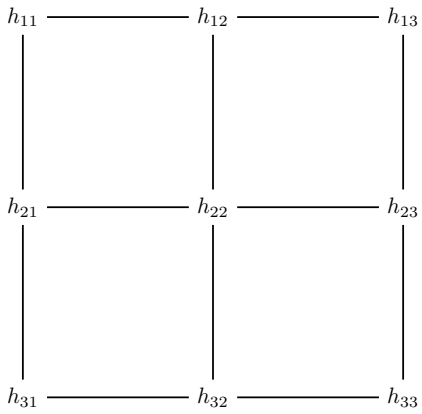

Figure 3.1: Each row and each column represents an isotropic subspace of dimension 2. Note that the diagram does not contain all edges of the orthogonality graph.

(1) $h_{ij} \cdot h_{i+1,j}, \quad h_{ij} \cdot h_{i,j+1} = 0$

(2) $h_{ij} \cdot h_{i+1,j+1} = 1$

(3) $h_{ij} + h_{i+1,j} = h_{i+1,j}, \quad h_{ij} + h_{i,j+1} = h_{i,j+2}$.

For an illustration see Figure 3.1. Observe that the set $\boxplus$ is CAO due to its definition and that f is constant on each row, respectively column, i.e.,

$$f(h_{ij}, h_{i,j+1}) = f(h_{ij}, h_{i,j+2}) = f(h_{i,j+1}, h_{i,j+2})$$

for all $j \in \{1,2,3\}$ and each row indexed by $i \in \{1,2,3\}$ and analogously for each column.

For deducing conditions on $t^\circ \in \mathcal{B}^f$ arising from $\boxplus$ we will require a technical lemma:

Lemma 3.2.4. *Let $k \geq 2$, K be CAO and $a : K \to \mathbb{R}$ with $\boxplus \subset \operatorname{supp}\{a\}$. Set $a_{ij} = a(h_{ij})$ for $h_{ij} \in \boxplus$ and assume that $|a_{ij}| = |a_{ji}|$ and $a_{ij} \neq 0$ for all $i, j \in \{1,2,3\}$. Furthermore, assume that the following relations hold:*

$$a_{32} = f(h_{22}, h_{12}) \cdot a_{22} \cdot a_{12}, \tag{3.13}$$

$$a_{23} = f(h_{22}, h_{21}) \cdot a_{22} \cdot a_{21}, \tag{3.14}$$

$$a_{11} = \underbrace{f(h_{11}, h_{21})}_{=f(h_{21},h_{31})} \cdot a_{21} \cdot a_{31} = \underbrace{f(h_{11}, h_{12})}_{=f(h_{12},h_{13})} \cdot a_{12} \cdot a_{13}. \tag{3.15}$$

Then

$$f(h_{31}, h_{32}) \cdot a_{31} \cdot a_{32} = -f(h_{13}, h_{23}) \cdot a_{13} \cdot a_{23}. \tag{3.16}$$

The lemma is formulated more general as necessary because it will become important in this form in the subsection about *integral vertices of* Q_k^f.

Proof. We simply expand the the LHS and RHS of (3.16) and compare the occurring factors. Using the bilinearity of f we compute for the LHS

$$\begin{aligned}
&f(h_{31},h_{32})\cdot a_{31}\cdot a_{32}\\
=&f(\underbrace{h_{11}+h_{21}}_{=h_{31}},\underbrace{h_{12}+h_{22}}_{h_{32}})\cdot \underbrace{f(h_{11},h_{21})\cdot\frac{a_{11}}{a_{21}}}_{=a_{31},\text{ due to (3.15)}}\cdot\underbrace{f(h_{22},h_{12})\cdot a_{22}\cdot a_{12}}_{=a_{32},\text{ due to (3.13)}}\\
=&f(h_{11},h_{12})\cdot f(h_{11},h_{22})\cdot f(h_{21},h_{12})\cdot f(h_{21},h_{22})\cdot f(h_{11},h_{21})\cdot f(h_{22},h_{12})\cdot\left(a_{11}\cdot a_{22}\cdot\frac{a_{12}}{a_{21}}\right)
\end{aligned}$$

and for the RHS

$$\begin{aligned}
&f(h_{13},h_{23})\cdot a_{13}\cdot a_{23}\\
=&f(\underbrace{h_{11}+h_{12}}_{=h_{13}},\underbrace{h_{21}+h_{22}}_{h_{23}})\cdot\underbrace{f(h_{11},h_{12})\frac{a_{11}}{a_{12}}}_{=a_{13},\text{ due to (3.15)}}\cdot\underbrace{f(h_{22},h_{21})\cdot a_{22}\cdot a_{21}}_{=a_{32},\text{ due to(3.14)}}\\
=&f(h_{11},h_{21})\cdot f(h_{11},h_{22})\cdot f(h_{12},h_{21})\cdot f(h_{12},h_{22})\cdot f(h_{11},h_{12})\cdot f(h_{22},h_{21})\cdot\Big(a_{11}\cdot a_{22}\cdot\underbrace{\frac{a_{21}}{a_{12}}}_{=\frac{a_{12}}{a_{21}}}\Big)\\
=&f(h_{11},h_{12})\cdot f(h_{11},h_{22})\cdot(-f(h_{21},h_{12}))\cdot f(h_{21},h_{22})\cdot f(h_{11},h_{21})\cdot f(h_{22},h_{12})\\
&\cdot\left(a_{11}\cdot a_{22}\cdot\frac{a_{12}}{a_{21}}\right)\\
=&-f(h_{31},h_{32})\cdot a_{31}\cdot a_{32},
\end{aligned}$$

where we used that $f(h_{12},h_{21})=-f(h_{21},h_{12})$ since $h_{12}\cdot h_{21}=1$. □

The lemma enables us to characterize the mentioned "forbidden" substructures in the graph $G((\operatorname{supp}\{t^\circ\}))$ with $t^\circ\in\mathcal{B}^f$.

Lemma 3.2.5. *Let $k\geq 2$, $K\subset\mathbb{F}_2^{2n}$ be CAO and $t^\circ:K\to\{0,1,-1\}$. Furthermore, suppose that the graph $G((\operatorname{supp}\{t^\circ\}^*))$ contains an induced $4-$cycle, i.e., there are $h_{11},h_{21},h_{12},h_{22}\in\operatorname{supp}\{t^\circ\}\cap\boxplus$ for $\boxplus\subset\mathbb{F}_2^{2n}$ defined as in Definition 3.2.3. Then $t^\circ\notin(Q_k^f(K))^\circ$*

Crucial for the proof is to notice that the assumptions (3.13), (3.14) and (3.15) of Lemma 3.2.4 have the same form as Condition (A2) if $t^\circ:K\to\{0,1,-1\}$ and $h_{11},h_{12},h_{21},h_{22}\in\operatorname{supp}\{t^\circ\}$.

Proof. We will prove the statement by contradiction. Suppose that there is $t^\circ\in\mathcal{B}^f(K)$ and $\boxplus\subset\mathbb{F}_2^{2n}$ with $h_{11},h_{21},h_{12},h_{22}\in\operatorname{supp}\{t^\circ\}\cap\boxplus$. Then, due to the construction of $\boxplus$, the subgraph $G(\{h_{11},h_{21},h_{12},h_{22}\})$ is a cycle of four vertices (see Figure 3.2). Applying Theorem 3.2.2, Condition (A2) has to hold for t° and the set $\operatorname{supp}\{t^\circ\}$ has to be CAO which implies

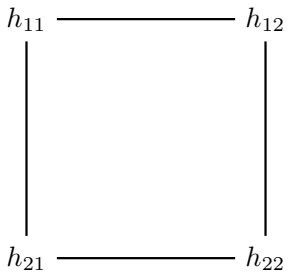

Figure 3.2: The initial setting for the constructed contradiction in Lemma 3.2.5.

$\boxplus \subset \text{supp}\{t^\circ\}$, so $h_{33} \in \text{supp}\{t^\circ\}$. Expanding $t(h_{33})$ by the bottom row and the most right column of Figure 3.1 we obtain

$$f(h_{31}, h_{32}) \cdot t^\circ(h_{31}) \cdot t^\circ(h_{32}) = t^\circ(h_{33}) = f(h_{13}, h_{23}) \cdot t^\circ(h_{13}) \cdot t^\circ(h_{23})$$

but since all assumptions of Lemma 3.2.4 are satisfied (3.16) holds, thus

$$f(h_{31}, h_{32}) \cdot t^\circ(h_{31}) \cdot t^\circ(h_{32}) = -f(h_{13}, h_{23}) \cdot t^\circ(h_{13}) \cdot t^\circ(h_{23}),$$

forcing $t^\circ(h_{33}) = 0$ which is a contradiction to $h_{33} \in \text{supp}\{t^\circ\}$. □

We will meet the diagram $\boxplus$ of Figure 3.1 again in the subsequent sections. Such a square often arises in quantum physics and it can be used to describe a phenomenon that divides classical from quantum mechanics, namely *contextuality*. We will investigate this connection in further detail in Section 3.3.

Every induced 4−cycle free subgraph $G(\text{supp}\{t^\circ\})$ for $t^\circ \in \mathcal{B}^f$ induces much "isotropic" related structure to the set $\text{supp}\{t^\circ\}$.

Corollary 3.2.6. *Let $k \geq 2$, $K \subset \mathbb{F}_2^{2n}$ be CAO, $t^\circ \in \mathcal{B}^f(K)$ and let $h \in \text{supp}\{t^\circ\}$. Then at least one of the two statements hold:*

1. *The set* $\text{supp}\{t^\circ\} \cap \{h\}^\perp$ *is an isotropic subspace.*
2. $\text{supp}\{t^\circ\} \subset \{h\}^\perp$

Proof. Let $t^\circ : K \to \{0, 1, -1\}$ and $h \in \text{supp}\{t^\circ\}$. We first note that $H := \text{supp}\{t^\circ\} \cap \{h\}^\perp$ not being an isotropic subspace means that $H \nsubseteq H^\perp$ or it is isotropic but not closed (consequently, not CAO). If the latter is the case, then $\text{supp}\{t^\circ\}$ is not CAO because $\{h\}^\perp$ is closed under addition (hence CAO) as it is a subspace. Then t° violates constraint (A2) and $t^\circ \notin \mathcal{B}^f(K)$ due to Theorem 3.2.2.

For the remaining cases we assume that there are $a_1, a_2 \in H$ (thus, $a_1 \cdot h = a_2 \cdot h = 0$) such that a_1, a_2 are not orthogonal to each other, i.e., $a_1 \cdot a_2 = 1$, and $b \in \text{supp}\{t^\circ\} \setminus \{h\}^\perp$,

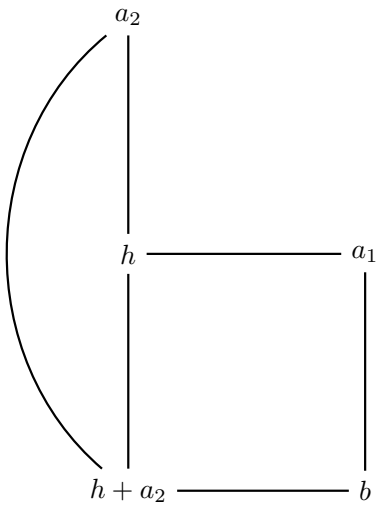

Figure 3.3: The graph $G(\{a_2, h, a_1, h + a_2, b\})$ for case 2. in the proof of Corollary 3.2.6.

i.e., $h \cdot b = 1$. This is equivalent to H being not isotropic and $\text{supp}\{t^\circ\} \not\subseteq \{h\}^\perp$. If we are able construct an induced $4-$cycle in $G(\text{supp}\{t^\circ\})$, Lemma 3.2.5 implies that $t^\circ \notin \mathcal{B}^f(K)$ and we have proved the statement by contraposition.

So, now assume that H is CAO (otherwise we are done due to the first observation). We have to distinguish three cases with respect to the orthogonality relations of a_1 and a_2 to b:

1. $a_1 \cdot b = a_2 \cdot b = 0$. Then, we have a $4-$cycle in $G(\text{supp}\{t^\circ\})$ with vertices $\{h, a_1, a_2, b\}$.

2. b is orthogonal to exactly one of the elements a_1, a_2, without loss of generality $a_1 \cdot b = 0, a_2 \cdot b = 1$. In this case the points $h, a_1, h + a_2, b$ form a $4-$cycle (see Figure 3.2).

3. $a_1 \cdot b = a_2 \cdot b = 1$. Here, $\{h, a_1 + h, a_2 + h, b\}$ form a $4-$cycle.

Hence, we showed that the negation of the two statements always forces that $t^\circ \notin \mathcal{B}^f(K)$ which finishes the proof by contraposition. □

We are now ready to completely characterize the sets $\text{supp}\{t^\circ\}$ for $t^\circ : K \to \{0, 1, -1\}$ and $t^{\circ,*} \in (Q_k^f(K))^\circ$. Therefore, we define the following subset of the power set of $\mathbb{F}_2^{2n}$:

Definition 3.2.7. Let

$$\mathcal{K} := \Big\{ K \subset \mathbb{F}_2^{2n} \,|\, K = H \dot\cup (h_1 + H) \dot\cup \ldots \dot\cup (h_\ell + H),\ H \text{ isotropic subspace}, \\ h_1, ..., h_\ell \in H^\perp, h_i \cdot h_j = 1 \text{ for all } 1 \le i, j \le n, i \ne j \Big\}. \tag{3.17}$$

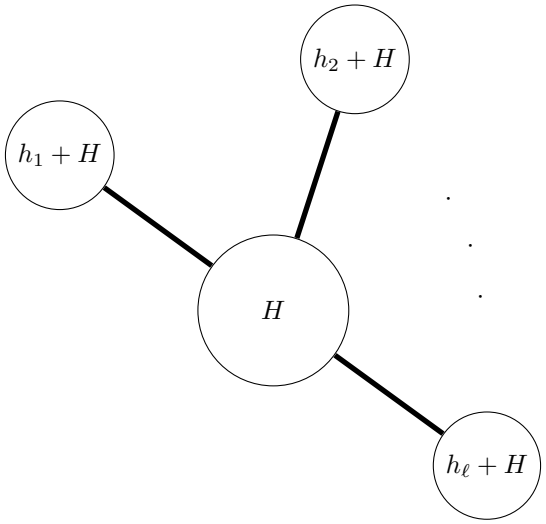

Figure 3.4: The structure of the orthogonality graph for $G(K)$ with $K \in \mathcal{K}$. Each set $H \cup (h_i + H)$ is clique and each set $h'_1, ..., h'_\ell$ with $h'_i \in h_i + H$ an independent set.

As we will see in the next theorem the sets in $\mathcal{K}$ coincide with the accessible sets $\text{supp}\{t^\circ\} \subset \mathbb{F}_2^{2n}$ for $t^\circ \in \mathcal{B}^f$. The underlying orthogonality graph for $K \in \mathcal{K}$ is given in Figure 3.4. Note that $\mathcal{K}$ does not coincide with the set of CAO subsets of $\mathbb{F}_2^{2n}$, e.g., $\boxplus$ is CAO but $\boxplus \notin \mathcal{K}$.

Example 3.2.8 Let $K = \{x_1, x_2, x_1x_2, y_2, x_1y_2, z_2, x_1z_2\} \subset \mathbb{F}_2^4$ and define $t^\circ : \mathbb{F}_2^4 \to \{0, 1, -1\}$ by

$$t^\circ(h) = \begin{cases} 1, & \text{if } h \in K \\ 0, & \text{otherwise.} \end{cases}$$

Note that we have

$$\text{supp}\{t^\circ\} = H \cup (x_2 + H) \cup (y_2 + H) \cup (z_2 + H),$$

where $H = \{x_1, 0\}$. The underlying graph of $\text{supp}\{a\}$ is given in Figure 3.2.

Theorem 3.2.9. *Let $k \geq 2$, $K \subset \mathbb{F}_2^{2n}$ be CAO and $t^\circ : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$. If $t^\circ \in \mathcal{B}^f(K)$, then* $\text{supp}\{t^\circ\} \in \mathcal{K}$.

Proof. Let $t^\circ \in \mathcal{B}^f(K)$ and let $h_1, \ldots, h_\ell \in \text{supp}(t^\circ)$ be maximal with respect to the index ℓ,

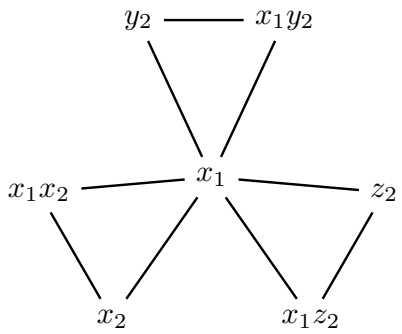

Figure 3.5: The graph $G(\text{supp}\{t^\circ\}^*)$ for t° in Example 3.2.8. The graph does not contain an induced 4−cycle.

not inclusion maximal, satisfying $h_i \cdot h_j = 1$ for all $i \neq j$. Then

$$\text{supp}\{t^\circ\} = (\{h_1\}^\perp \cap \text{supp}\{t^\circ\}) \cup \ldots (\{h_\ell\}^\perp \cap \text{supp}\{t^\circ\}) \tag{3.18}$$

since this forces that every element $h \in \text{supp}\{t^\circ\}$ has to be orthogonal to at least one h_i (otherwise $h_1, ..., h_\ell$ cannot be maximal). We distinguish two cases:

1. $\ell = 1$:
   Then $\text{supp}\{t^\circ\} \subset \{h_1\}^\perp$ and due to the maximality of ℓ, $\text{supp}\{t^\circ\}$ is isotropic as well. Moreover, since $t^\circ \in \mathcal{B}^f(K)$ the set $\text{supp}\{t^\circ\}$ is CAO and thus, $\text{supp}\{t^\circ\}$ is an isotropic subspace. Now, if $\dim(\text{supp}\{t^\circ\}) = k$, choose any $(k-1)$-dimensional subspace H with $h_1 \notin H$ and $\text{supp}\{t^\circ\} = H \cup (h_1 + H)$.

2. $\ell \geq 2$:
   Let

   $$H = \{h_1\}^\perp \cap \{h_2\}^\perp \cap \text{supp}\{t^\circ\}.$$

   We will prove that this is the H of (3.17). Since $h_i \cdot h_j = 1$ for all $i \neq j$, we have $\text{supp}\{t^\circ\} \not\subseteq \{h_i\}^\perp$ and the last lemma implies that $\text{supp}\{t^\circ\} \cap \{h_i\}^\perp$ is an isotropic subspace for all $i = 1, ..., \ell$. Hence, H is an isotropic subspace as the intersection of isotropic subspaces. For $\ell \geq 3$ we will show that

   $$H = \{h_1\}^\perp \cap \{h_2\}^\perp \cap \{h_3\}^\perp \cap \text{supp}\{t^\circ\}$$

   by contradiction.
   Assume that there is $h \in \Big(\{h_1\}^\perp \cap \{h_2\}^\perp \cap \text{supp}\{t^\circ\}\Big) \setminus \{h_3\}^\perp$. This means that $h \cdot h_1 = h \cdot h_2 = 0$ but $h \cdot h_3 = 1$. Since $\text{supp}\{t^\circ\}$ has to be CAO, it follows that $h_1 + h$, $h_2 + h \in \{h_3\}^\perp \cap \text{supp}\{t^\circ\}$ but $(h_1+h)\cdot(h_2+h) = h_1 \cdot h_2 = 1$, so the intersection $\{h_3\}^\perp \cap \text{supp}\{t^\circ\}$

cannot be not isotropic and we get $t^\circ \notin \mathcal{B}^f(K)$ due to the last lemma, a contradiction. Alternatively, we can argue that $G(\mathrm{supp}\{t^\circ\})$ contains the induced subgraph generated by the vertices h_1, h_1+h, h_3, h_2+h_3+h forming an induced 4-cycle. Continuing in the same fashion for $h_4, ..., h_\ell$ we can iteratively deduce that

$$\begin{aligned} H = \{h_1\}^\perp \cap \{h_2\}^\perp \cap \cdots \cap \{h_\ell\}^\perp \cap \mathrm{supp}\{t^\circ\} &= \{h_1\}^\perp \cap \{h_2\}^\perp \cap \mathrm{supp}\{t^\circ\} \\ &= \{h_i\}^\perp \cap \{h_j\}^\perp \cap \mathrm{supp}\{t^\circ\} \end{aligned}$$

for all $1 \leq i \neq j \leq \ell$.
It remains to analyze the exact structure of $\{h_i\}^\perp \cap \mathrm{supp}\{t^\circ\}$. Recall that H can be expressed as the intersection of the orthogonal complements $\{h_1\}^\perp$ and $\{h_2\}^\perp$ with $\mathrm{supp}\{t^\circ\}$. We will fix $i = 1$ and set $\{h_1\}^\perp \cap \mathrm{supp}\{t^\circ\} = \mathrm{span}\{h_1, a_1 \dots a_s\}$. By observing that $\mathrm{span}\{h_1, a_1, \dots, a_s\} = \mathrm{span}\{h_1, h_1+a_1, \dots h_1+a_s\}$ and either $a_i \in H$ or $h_1+a_i \in H$ (since either $a_i \in \{h_2\}^\perp$ or $(h_1+a_i) \in \{h_2\}^\perp$ since we have $(h_1+a_i)\cdot h_2 = 0$ if $a_i \cdot h_2 = 1$) we may choose the basis elements $a_1, ..., a_s \in H$ and it follows $\{h_1\}^\perp \cap \mathrm{supp}\{t^\circ\} = \mathrm{span}\{h_1, H\} = H \cup (h_1 + H)$. By equation (3.18), we conclude that

$$\mathrm{supp}\{t^\circ\} = H \dot\cup (h_1 + H) \dot\cup \dots \dot\cup (h_\ell + H).$$

□

Conversely, if we are given a set $K = H \cup (h_1 + H) \cup \cdots \cup (h_\ell + H) \in \mathcal{K}$, we can easily construct $t^\circ \in \mathcal{B}^f$ such that $\mathrm{supp}\{t^\circ\} = K$. Before analyzing the general construction we consider the following example:

Example 3.2.10 Let f be defined as in (2.3) and consider $t^\circ \in \mathcal{B}^f$ with support $\mathrm{supp}\{t^\circ\} = \{H, x_3 + H, y_3 + H, z_3 + H\}$, where $H = \{0, x_1x_2, y_1y_2, z_1z_2\}$. We fix the assignments $t^\circ(x_1x_2) = t^\circ(z_1z_2) = t^\circ(x_3) = t^\circ(z_3) = 1$ and $t^\circ(y_1y_2) = t^\circ(y_3) = -1$, ensuring $t^\circ_{|H} \in \mathcal{A}_2^f$. Note that we have $f(x_3, h) = f(y_3, h) = f(z_3, h) = 1$ for all $h \in H$.

This completely determines t° since for any $h \in H$ the assignments on the cosets are $t^\circ(x_3+h) = f(x_3, h)\cdot t^\circ(x_3)\cdot t^\circ(h) = t^\circ(h) = t^\circ(z_3+h)$ and $t^\circ(y_3+h) = f(y_3, h)\cdot t^\circ(y_3)\cdot t^\circ(h) = -t^\circ(h)$.

If $\dim(H) = k$, we fix an arbitrary $t \in \mathcal{A}_k^f(H)$ (implying that $\mathrm{supp}\{t\} = H$). We construct t° as follows:
Set $t^\circ(h) = t(h)$ for all $h \in H$. For all $h_1, ..., h_\ell$ choose $t^\circ(h) \in \{1, -1\}$. This determines the values on the cosets $h_i + H$ since for $h_i + h \in h_i + H$, $h \in H$ we have $t^\circ(h_i + h) = f(h, h_i) \cdot t^\circ(h_i) \cdot t(h)$. To show that t° satisfies condition(A2) on the whole set K we consider arbitrary orthogonal $h, h' \in K$. If $h, h' \in H$, then $h + h' \in H$ and due to $t \in \mathcal{A}_k^f(H)$ we have

$$t^\circ(h + h') = t(h + h') = f(h, h') \cdot t(h) \cdot t(h') = f(h, h') \cdot t^\circ(h) \cdot t^\circ(h').$$

If $h \in H$ and $h' \in h_i + H$ for some $i \in \{1, ..., \ell\}$, then $h' = h_i + h''$ for some $h'' \in H$ and using bilinearity and symmetry for orthogonal elements of f it holds

$$\begin{aligned} t^\circ(h + h') = t^\circ(h_i + (h + h'')) &= f(h_i, h + h'') \cdot t^\circ(h_i) \cdot t^\circ(h + h'') \\ &= f(h_i, h) \cdot f(h_i, h'') \cdot f(h, h'') \cdot t^\circ(h_i) \cdot t^\circ(h) \cdot t^\circ(h'') \\ &= f(h_i + h'', h) \cdot f(h_i, h'') \cdot t^\circ(h_i) \cdot t^\circ(h) \cdot t^\circ(h'') \\ &= f(h_i + h'', h) \cdot t^\circ(h_i + h'') \cdot t^\circ(h) \\ &= f(h, h') \cdot t^\circ(h) \cdot t^\circ(h'). \end{aligned}$$

If $h_i + h, h_i + h' \in h_i + H$ (so $h, h' \in H$), then once again bilinearity and symmetry for orthogonal elements of f yields

$$\begin{aligned} & t^\circ((h_i + h) + (h_i + h')) \\ =& t^\circ(h, h') \\ =& f(h, h') \cdot t(h) \cdot t^\circ(h') \\ =& f(h, h') \cdot \big(f(h_i, h) \cdot f(h_i, h)\big) \cdot \big(f(h_i, h') \cdot f(h_i, h')\big) \cdot \big(t^\circ(h_i) \cdot t^\circ(h_i)\big) \cdot t^\circ(h) \cdot t^\circ(h') \\ =& f(h_i + h, h_i + h') \cdot t^\circ(h_i + h) \cdot t^\circ(h_i + h'). \end{aligned}$$

If $h \in h_i + H$ and $h' \in h_j + H$ for some $i \neq j$, then h and h' are not orthogonal to each other. Thus, we have considered all possible orthogonality relations between h and h' and have constructed $t^\circ \in \mathcal{B}^f$. Analogously to Proposition 3.1.2 (i) we have:

Proposition 3.2.11. *Let $t^\circ \in \mathcal{B}^f$ with $K = H \cup (h_1 + H) \cup \cdots \cup (h_\ell + H) = \operatorname{supp}\{t^\circ\}$ and $H_i = H \cup (h_i + H)$ for $i = 1, ..., \ell$. It holds*

$$\begin{aligned} & \{(t^\circ)' \in \mathcal{B}^f \,|\, \operatorname{supp}\{(t^\circ)'\} = K\} \\ =& \{\eta t^\circ \,|\, \eta_{|H_i} : H_i \to \{1, -1\} \text{ is a character on the additve group } H_i,\ i = 1, ..., \ell\}. \end{aligned}$$

Integral vertices of $(Q_k^f)^\circ$

Having characterized the structure of $\operatorname{supp}\{t^\circ\}$ for $t^\circ \in \mathcal{B}^f$ we are able to show that if the set $\operatorname{supp}\{t^\circ\}$ is inclusion maximal in $\mathcal{B}^f$, then $t^{\circ,*}$ is a vertex of $(Q_k^f)^\circ$ and thus defines a facet normal of Q_k^f. The idea is to show that every such $t^{\circ,*}$ cannot be written as a proper convex combination of elements in $(Q_k^f)^\circ$. Hence, it is an extreme point and therewith a vertex of $(Q_k^f)^\circ$. This result cannot be simply extended to $K \subset \mathbb{F}_2^{2n}$ being CAO. However, in the next section we will show that if $K \in \mathcal{K}$ then the projected polytope $Q_k^f(K)$ is reflexive (i.e., the dual polytope is integral).

In order to prove that certain integral functions in the dual polytope are vertices we need a generalization of Theorem 3.2.2 for "partially" integral functionals in the dual polytope. If $a : K \to \mathbb{R}$, we will write a^* for $a_{|K^*}$.

Lemma 3.2.12. *Let $k \geq 2$, $K \subset \mathbb{F}_2^{2n}$ be CAO and $a : K \to \mathbb{R}$ with $a^* \in (Q_k^f(K))^\circ$ and let $|a(h)| = 1$ for some $h \in K$. Then*

$$a(h + h') = f(h, h') \cdot a(h) \cdot a(h') \tag{3.19}$$

for all $h' \in K$ such that $h \cdot h' = 0$ and $h' \in \operatorname{supp}\{a\}$.

Note that (3.19) is a generalization of (A2) since we just require that $|a(h)| = 1$ for all tuples of orthogonal elements $h, h' \in K$ with $|a(h)|, a(h')| > 0$.

Proof. Suppose that the assumptions of the theorem hold and let $h'' = h + h'$. Let $t \in A_2^f(K)$ with $\operatorname{supp}\{t\} = \{0, h, h', h''\}$. Since $a^* \in (Q_k^f(K))^\circ$, we have

$$t(h)a(h) + t(h')a(h') + t(h'')a(h'') \geq -1.$$

If we fix $t(h) = -a(h)$, this translates to

$$t(h')a(h') + t(h'')a(h'') \geq 0$$

and due to $t(h'') = f(h, h') \cdot t(h) \cdot t(h') = -f(h, h') \cdot a(h) \cdot t(h')$ (Condition (A2) for t) we obtain

$$\underbrace{\Big(- f(h, h') \cdot a(h) \cdot t(h') \Big)}_{\in \{1, -1\}} \cdot a(h'') \geq -t(h') \cdot a(h').$$

Now we can choose $t(h') \in \{1, -1\}$ and if we multiply by $-f(h, h') \cdot a(h) \cdot t(h')$, we get $a(h'') \leq f(h, h') \cdot a(h) \cdot a(h')$ for one of the cases and for the other $a(h'') \geq f(h, h') \cdot a(h) \cdot a(h')$, so

$$a(h'') = f(h, h') \cdot a(h) \cdot a(h').$$

□

Our goal for the subsection is to prove the following theorem:

Theorem 3.2.13. *Let $k \geq 2$, $t^\circ \in \mathcal{B}^f$ and $\operatorname{supp}\{t^\circ\} = H \dot\cup (h_1 + H) \dot\cup \ldots \dot\cup (h_\ell + H) \in \mathcal{K}$, where H is an isotropic subspace of dimension k, $h_1, \ldots h_\ell \in H^\perp$ and $h_i \cdot h_j = 1$ for all $i \neq j$. If the chain $h_1, \ldots, h_\ell$ is of maximal length in $H^\perp$, then $t^{\circ,*}$ is a vertex of Q_k^f.*

The set $\operatorname{supp}\{t^\circ\}$ described in the theorem is inclusion maximal, meaning that there is no other integral functional $(t^\circ)' \in \mathcal{B}^f$ such that $\operatorname{supp}\{t^\circ\} \subsetneq \operatorname{supp}\{(t^\circ)'\}$. After the proof of the theorem we will explain how these sets look like by using the properties about $\mathbb{F}_2^{2n}$ derived in subsection 2.2. Moreover, if $t^{\circ,*}$ is a vertex of $(Q_k^f)^\circ$, it gives rise to a facet normal of Q_k^f. Once again, this result holds for all $2 \leq k \leq n$.

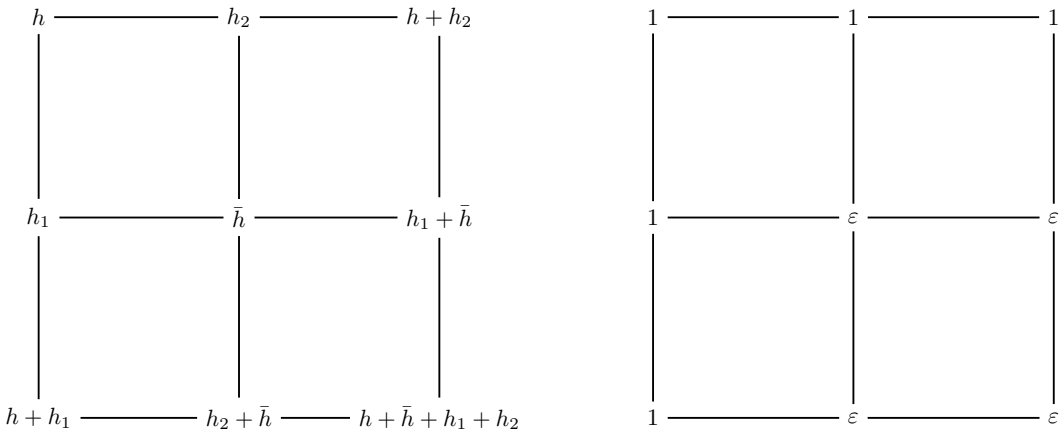

Figure 3.6: Illustration of the setup in case 1.1. The right part indicates the absolute values of x_1 that have to be assigned to the positions indicated on the left.

The idea of the proof is to assume that we can write such a t° as a proper convex combination, that is $t^{\circ,*} = \lambda a_1^* + (1-\lambda)a_2^*$ with $0 < \lambda < 1$ and then to show that one of the points a_1^*, a_2^* cannot lie in $(Q_k^f)^\circ$. Therefore, we aim to construct $\boxplus \subset \operatorname{supp}\{a_1\}$ where $\boxplus$ is defined as in Definition 3.2.3 and then to apply Lemma 3.2.4 to a_1.

Proof of Theorem 3.2.13. Suppose that the assumption of the theorem holds for t°. and assume $t^{\circ,*} = \lambda a_1^* + (1-\lambda)a_2^*$ for $0 < \lambda < 1$ and $a_1, a_2 : \mathbb{F}_2^{2n} \to \mathbb{R}$ with $a_1^*, a_2^* \in (Q_k^f)^\circ$ and $a_1(0) = a_2(0) = 1$. Since $|a_i(h)| \leq 1$ for all $h \in \mathbb{F}_2^{2n}$, we have $\lambda|a_1^*(h)| + (1-\lambda)|a_2^*(h)| \leq 1$ for all $h \in (\mathbb{F}_2^{2n})^*$ and equality is given if and only if $|a_1^*(h)| = |a_2^*(h)| = 1$. Thus, it must hold $a_1^*(h) = a_2^*(h) = t^\circ(h)$ whenever $|t(h)| = 1$ (i.e., $h \in \operatorname{supp}\{t^\circ\}$). This forces $\operatorname{supp}\{t^\circ\} \subsetneq \operatorname{supp}\{a_i\}$ because for being a proper convex combination we require $\bar{h} \in \operatorname{supp}\{a_i\} \setminus \operatorname{supp}\{t^\circ\}$ for $i = 1, 2$. Let $|a_1(\bar{h})| = \varepsilon > 0$.

We analyze the orthogonality relations of $\bar{h}$ with $\operatorname{supp}\{t^\circ\}$. Let $\dim(H^\perp/H) = 2(n - \dim(H)) = m$. Then, due to Lemma 2.2.9 the longest chain of mutually non-orthogonal elements in $H^\perp$ has length $\ell = m + 1$. To do so, we distinguish two cases:

1. $\bar{h} \notin H^\perp$:
   This means that there is $h \in H$ such that $h \cdot \bar{h} = 1$. The maximal dimension for H is $n-1$ (in this case the sets $H \cup h_i + H$, $i = 1, ..., \ell$, are isotropic subspaces of dimension n), so $\ell \geq 3$. Since we have $\bar{h} \cdot h_i = 0$ or $\bar{h} \cdot (h + h_i) = 0$ and $h + h_i \in \operatorname{supp}\{t^\circ\} \subsetneq \operatorname{supp}\{a\}$ for all $i = 1, ..., \ell$, we may assume without loss of generality that $\bar{h} \cdot h_1 = \bar{h} \cdot h_2 = 0$. The elements $h, h_1, h_2, \bar{h}$ form a $4-$cycle in $G(\operatorname{supp}\{a_1\})$.

   By applying Lemma 3.2.12 there is $\boxplus$ with $h, h_1, h_2, \bar{h} \in \boxplus$ and $\boxplus \subset \operatorname{supp}\{a_1\}$ where the necessary absolute values for the elements in $\boxplus$ are shown in Figure 3.6. Now, all

assumptions of Lemma 3.2.4 are met as we have symmetry of absolute values and

$$\begin{aligned} a(h_2+\bar{h}) &= f(h_2,\bar{h})\cdot a(\bar{h})\cdot a(h_2),\\ a(h_1+\bar{h}) &= f(h_1,\bar{h})\cdot a(\bar{h})\cdot a(h_1),\\ a(h) &= f(h,h_1)\cdot a(h_1)\cdot a(h+h_1) = f(h,h_2)\cdot a(h_2)\cdot a(h+h_2) \end{aligned}$$

coincide with equations (3.13),(3.14) and (3.15). Now,

$$f(h,h_i)\cdot a(h+h_i)\cdot a(h_j+\bar{h}) = a(h+\bar{h}+h_i+h_j) = f(h_i+\bar{h})\cdot a(h_i+\bar{h})\cdot a(h+h_j)$$

but Lemma 3.2.4 yields that

$$f(h,h_i)\cdot a(h+h_i)\cdot a(h_j+\bar{h}) = -f(h_i+\bar{h})\cdot a(h_i+\bar{h})\cdot a(h+h_j),$$

forcing $a(h+\bar{h}+h_i+h_j)=0$, a contradiction.

2. $\bar{h}\in H^{\perp}$:
   This case is more tricky. If $\dim H = n-1$, then $\dim H^{\perp} = n+1$ and $\ell = 3$. Moreover, $H^{\perp} = H\cup(h_1+H)\cup(h_2+H)\cup((h_1+h_2)+H)$ with $h_1\cdot h_2 = 1$ is a closed subspace and we obtain $\operatorname{supp}\{t^{\circ}\} = H^{\perp}$ and $\bar{h}\in H^{\perp}\setminus\operatorname{supp}\{t^{\circ}\}$ is not possible.

   Thus, it has to hold $\dim(H) < n-1$. In this case the minimal length of a non orthogonal chain is 5 (note that we require $k\geq 2$ here), so we consider $\ell\geq 5$. As we have seen in Lemma 2.2.9 we can write $H^{\perp} = \operatorname{span}\{H,h_1,...,h_{\ell-1}\}$ and since $\bar{h}\notin H$, we may choose $h_1,...,h_{\ell}$ in such a way that $\bar{h}\in\operatorname{span}\{h_1,...,h_{\ell-1}\}$ (this means that we replace h_i by h_i+h' for some $h'\in H$ if necessary). Observe that we have $\sum_{i=1}^{\ell-1}h_i = h_{\ell}$ and $\ell-1$ is even.

   We assume without loss of generality that $\bar{h} = \sum_{i\in I}h_i$ for $I=\{1,...,s\}$. If $|I|$ is even, we have $s<\ell-2$ because of $\bar{h}\neq h_{\ell}$. Then, $\bar{h}\cdot h_j = 0$ for all $j = s+1,...,\ell$ and $\bar{h}\cdot h_j = 1$ for $j=1,...,s$. So, $\bar{h}$ is orthogonal to at least two elements (e.g., $h_{\ell-1},h_{\ell}$) and non-orthogonal to at least one element (e.g., h_1). Similarly, if $|I|$ is odd, then $\bar{h}\cdot h_j = 0$ for all $j=1,...,s$, where s is at least 3, and $\bar{h}\cdot h_j = 1$ for all $j=s+1,...,\ell$, where $s<\ell$ (as $\bar{h}\neq 0 = \sum_{i=1}^{\ell}h_j$). Again, $\bar{h}$ is orthogonal to at least two elements (e.g., h_1,h_2) and non-orthogonal to at least one element (e.g., h_{ℓ}).

   If we assume without loss of generality that $\bar{h}\cdot h_1 = \bar{h}\cdot h_2 = 0$ and $\bar{h}\cdot h_3 = 1$, we can apply Lemma 3.2.12 and we are in the setting depicted in Figure 3.7. Once again, we

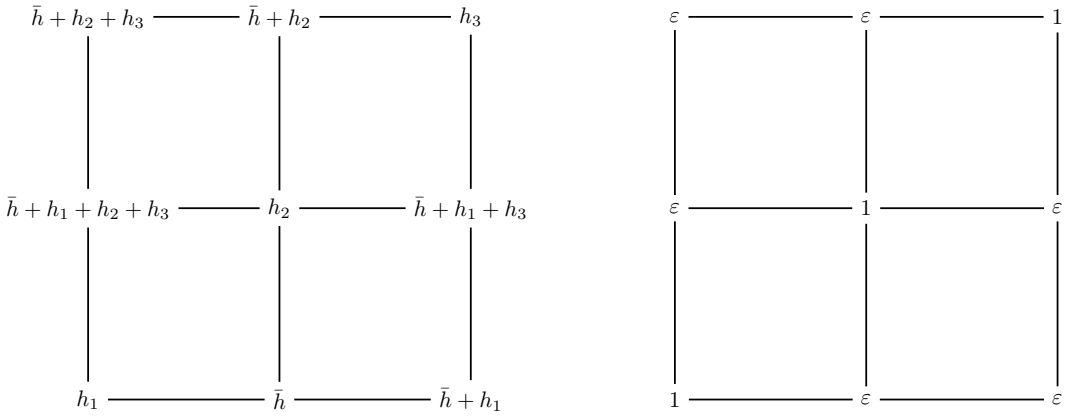

Figure 3.7: Illustration of case 2. By Lemma 3.2.12 the ones on the diagonal force that all other value assignments are non-zero.

have symmetry of the diagram and due to Lemma 3.2.12 we have

$$\begin{aligned} a(\bar{h}) &= f(h_2,\, \bar{h}+h_2)\cdot a(h_2)\cdot a(\bar{h}+h_2) \\ a(\bar{h}+h_1+h_3) &= f(h_2,\, \bar{h}+h_1+h_2+h_3)\cdot a(h_2)\cdot a(\bar{h}+h_1+h_2+h_3) \\ a(\bar{h}+h_2+h_3) &= f(\bar{h}+h_2+h_3,\, \bar{h}+h_1+h_2+h_3)\cdot a(\bar{h}+h_1+h_2+h_3)\cdot a(h_1) \\ &= f(\bar{h}+h_2+h_3,\, \bar{h}+h_2)\cdot a(\bar{h}+h_2)\cdot a(h_3), \end{aligned}$$

so the assumptions of Lemma 3.2.4 are satisfied. We have

$$f(h_1,h)\cdot a(h_1)\cdot a(\bar{h}) = a(\bar{h}+h_1) = f(h_3,\bar{h}+h_1+h_3)\cdot a(h_3)\cdot a(\bar{h}+h_1+h_3)$$

but, by Lemma 3.2.4, it has to hold

$$f(h_1,h)\cdot a(h_1)\cdot a(\bar{h}) = -f(h_3,\bar{h}+h_1+h_3)\cdot a(h_3)\cdot a(\bar{h}+h_1+h_3),$$

consequently, $a(\bar{h}+h_1)=0$, a contradiction.

Hence, in both cases we get a contradiction and $t^{\circ,*}$ cannot be written as a proper convex combination of points in $(Q_k^f)^\circ$. □

Remark 3.2.14 The proof cannot be simply translated to $(Q_k^f(K))^\circ$ for a CAO set $K\subset\mathbb{F}_2^{2n}$ since we required properties of the symplectic vector space $\mathbb{F}_2^{2n}$. An adaption of the proof would require a careful translation of these properties from $\mathbb{F}_2^{2n}$ to K.

If $K = H\cup(h_1+H)\cup\cdots\cup(h_\ell+H)\in\mathcal{K}$ for a k-dimensional isotropic subspace H, then $t^{\circ,*}\in(Q_k^f)^\circ$ with $t^\circ\in\mathcal{B}^f$ and $\operatorname{supp}\{t^\circ\}=K$ is a vertex of $(Q_k^f)^\circ$ if $\ell=2(n-k)+1$ due to

Lemma 2.2.9. We will show that this is also a necessary condition. Therefore, assume that $\ell < 2(n-k)+1$. We will show that t° can be written as a convex combination of elements in $\mathcal{B}^f$ (and $t^{\circ,*}$ as a convex combination of elements in $(Q_k^f)^\circ$). We distinguish two cases:

1. There is $h \in H^\perp \setminus K$ such that $h \cdot h_i = 1$ for all $i = 1, ..., \ell$. We define $t_1^\circ, t_2^\circ \in \mathcal{B}^f$ with $\mathrm{supp}\{t_1^\circ\} = \mathrm{supp}\{t_2^\circ\} = K \cup (h + H) \in \mathcal{K}$ by $(t_1)_{|K} = (t_2^\circ)_{|K} = t^\circ_{|K}$ and $t_1^\circ(h) = -t_2^\circ(h)$. This uniquely determines t_1°, t_2° since $t_i^\circ(h + h')$ for $h + h' \in h + H$, $h' \in H$ has to satisfy $t_i^\circ(h + h') = f(h, h') \cdot t_i^\circ(h) \cdot t_i^\circ(h')$ for $i = 1, 2$. Then $t^\circ = 1/2(t_1^\circ + t_2^\circ)$ and thus $t^{\circ,*}$ is not a vertex of $(Q_k^f)^\circ$.

2. If there is no element that can be added to $h_1, ..., h_\ell$ while preserving non-orthogonality, we are in the case that $h_\ell = h_1 + \cdots + h_{\ell-1}$ and $\ell < 2(n-k)$ (otherwise if $h_1, ..., h_\ell$ are linearly independent and $\ell < 2(n-k)$ we can always add an element until the corresponding cosets $h_1 + H, ..., h_\ell + H$ are a basis for $H^\perp/H$ (see Lemma 2.2.9)). Yet, in this case we can enlarge the isotropic subspace H to H' while preserving $h_1, ..., h_\ell \in H'$. The subspace

$$M = \{h' \in \mathbb{F}_2^{2n} \,|\, h' \cdot h = 0,\, h \in H,\, h' \cdot h_i = 0,\, i = 1, ..., \ell\}$$

has dimension $2^{2n-(k+\ell)}$ and contains H. Since

$$|M \setminus H| = 2^{2n-k-\ell} - 2^k \geq 2^{2n-k-(2(n-k)-1)} - 2^k = 2^{k+1} - 2^k > 0,$$

there exists $h' \in M \setminus H$ and we are able to extend H to $H' = H \cup (h' + H)$. In this case we define $t_1^\circ, t_2^\circ \in \mathcal{B}^f$ with $\mathrm{supp}\{t_i^\circ\} = H' \cup (h_1 + H') \cup \cdots \cup (h_\ell + H')$ and set $t_i^\circ(h) = t^\circ(h)$ for all $h \in K$ and $t_1^\circ(h') = -t_2^\circ(h')$. Then, once again, $t^\circ = t_1^\circ + t_2^\circ$.

We have seen that elements $t^\circ \in \mathcal{B}^f$ with inclusion maximal support give rise to facets of Q_k^f for all $k \geq 2$. The family of these facets is constant for all $2 \leq k \leq n$. One might ask if it is sufficient to fully describe Q_n^f:

Question 1.

$$Q_n^f \stackrel{?}{=} \{x : (\mathbb{F}_2^{2n})^* \to \{0, 1, -1\} \,|\, (t^{\circ,*})^T x \geq -1,\, t^\circ \in \mathcal{B}^f\} = (\mathrm{conv}\{t^{\circ,*} \,|\, t^\circ \in \mathcal{B}^f\})^\circ.$$

The inequalities on the RHS do not all induce facets of Q_n^f (respectively, they are not all vertices of the dual polytope). As we have shown before this would require to restrict on $t^\circ \in \mathcal{B}^f$ such that $\mathrm{supp}\{t^\circ\}$ is inclusion maximal.

Facets of SP_n as families of observables

So far, we have seen that there is a one-to-one correspondence between abelian subgroups in $\pm P_n \setminus \{-I\}$ with 2^k elements (respectively their associated projectors onto the common $+1$ eigenspace) and functions in $\mathcal{A}_k^f$. We will construct a similar correspondence between

families of Pauli observables and integral functions in $\mathcal{B}^f$ for f defined as in (2.3). Using the results of the last subsection this also enables us to construct facets of SP_n as families of Pauli observables in $\pm P_n$.

Let $(t^{\circ,*})^T x \geq -1$ with $t^\circ \in \mathcal{B}^f$ be an inequality that defines a face of Q_k^f. Then due to Theorem 3.2.9 we have

$$\mathcal{K} \ni K := \mathrm{supp}\{t^\circ\} = H \cup (h_1 + H) \cup \cdots \cup (h_\ell + H),$$

where H is an isotropic subspace, $h_1, ..., h_\ell \in H^\perp$ and $h_i \cdot h_j = 1$ for all $i \neq j$. We construct an associated set of observables $\mathcal{O}^K \subset \pm P_n$ as follows:

$$\mathcal{O}^K = \{g \in \pm P_n \,|\, r(g) \in K,\, \chi(g) = t^\circ(g)\}. \tag{3.20}$$

The set is constructed as the abelian subgroup in (3.6) and since t° satisfies (A2), it is therewith closed under the multiplication of commuting elements (which implies that $r(\mathcal{O}^K)$ is CAO). We obtain

$$\mathcal{O}^K = S \cup g_1 S \cup \cdots \cup g_\ell S,$$

where $S \subset \pm P_n$ is an abelian subgroup with $r(S) = H$ and $g_1, ..., g_\ell$ with $r(g_i) = h_i$ commute with all elements in S but mutually anticommute.

Example 3.2.15 Let t° be defined as in Example 3.2.10, that is to say, $K = \mathrm{supp}\{t^\circ\} = \{H, x_3 + H, y_3 + H, z_3 + H\}$, where $H = \{0, x_1x_2, y_1y_2, z_1z_2\}$, and assignments defined by $t^\circ(x_1x_2) = t^\circ(z_1z_2) = t^\circ(x_3) = t^\circ(z_3) = 1$ and $t^\circ(y_1y_2) = t^\circ(y_3) = -1$. Then, $S = \{X_1X_2, -Y_1Y_2, Z_1Z_2\}$ ensures that $\chi(g) = t^\circ(g)$ for all $g \in S$. The associated set $\mathcal{O}^K$ is

$$\mathcal{O}^\mathcal{K} = S \cup \{X_3 g \,|\, g \in S\} \cup \{-Y_3 g \,|\, g \in S\} \cup \{Z_3 g \,|\, g \in S\}.$$

Let $\mathcal{O}^K$ be as in (3.20) with corresponding $t^\circ \in \mathcal{B}^f$. The function t° is the image of $1/2^n \sum_{g \in \mathcal{O}^K} g$ under the linear map (3.4). Recall that it is defined as

$$\begin{aligned} \phi : \mathcal{H}_n &\to \{x \,|\, x : \mathbb{F}_2^{2n} \to \mathbb{R}\} \\ A &\mapsto t_A, \end{aligned}$$

where $t_A(r(g)) = \mathrm{Tr}\,(Ag)$ for $g \in P_n$. If $P_{S'} = 1/2^n \sum_{g' \in S'} g'$ is a projector onto a stabilizer

state, then

$$\begin{aligned}\operatorname{Tr}\left(P_{S'}\cdot\sum_{g\in\mathcal{O}^K}g\right)=\frac{1}{2^n}\sum_{g'\in S'}\sum_{g\in\mathcal{O}^K}\operatorname{Tr}(gg')&=\frac{1}{2^n}\sum_{g\in\mathcal{O}^K,g'\in S',g\in\{g',-g'\}}2^n\cdot\chi(g)\cdot\chi(g')\\&=\frac{1}{2^n}\sum_{h\in r(\mathcal{O}^K)\cap r(S)}2^n\cdot t_{P_{S'}}(h)\cdot t_K(h)\\&=(t^\circ)^T t_{P_{S'}}\\&=\begin{cases}|K\cap S'|,\ \text{if } t^\circ_{|S'}=(t_{P_{S'}})_{|S'}\\0,\ \text{otherwise.}\end{cases}\end{aligned}$$

Hence, we have the following theorem:

Theorem 3.2.16. *Let $\mathcal{M}$ be the set of all families $\mathcal{O}\subset\pm P_n$ of observables of the form $\mathcal{O}=S\cup g_1S\cup\ldots g_\ell S$ where $S\subset\pm P_n\setminus\{-I\}$ is an abelian subgroup and the g_i's commute with the elements in S but mutually anticommute, i.e., $g_ig_j=-g_jg_i$ for all $i\neq j$. Then it holds*

$$SP_n\subseteq\{A\in\ |\ Tr(A)=1,\ \sum_{O\in\mathcal{O}}Tr(AO)\geq 0\text{ for all }\mathcal{O}\in\mathcal{M}\}. \tag{3.21}$$

Additionally, if $\mathcal{O}\subset\mathcal{M}$ is inclusion maximal in $\mathcal{M}$, then $\sum_{O\in\mathcal{O}}Tr(AO)\geq 0$ defines a facet inequality of SP_n.

The proof follows from the last observations and Theorem 3.2.13. It establishes a one-to-one correspondence between functions in $\mathcal{B}^f$ and particular sets of observables. In the next section we will see that these sets have an interesting interpretation in quantum physics. Besides, if Question 1 can be answered with yes, we have equality in (3.21).

3.3 Contextuality related to Pauli observables and the polytope Q_k^f

In this section we will establish a connection between the characterized integral points in $(Q_k^f)^\circ$ (for $k\geq 2$) and *contextuality* with respect to Pauli observables. Contextuality is a feature that separates quantum mechanics from classical mechanics. One of its central aspects can be phrased as the following question:
If a measurement is performed, does it just simply reveal a predetermined outcome and is this outcome dependent upon other measurements?

We will explain the ideas of contextuality with the following gedankenexperiment, originally from [16]: Assume you sit in front of three boxes each hiding a black or a white ball and you are supposed to open two of them. You open one box after the other and after doing this several times you notice that you always uncover exactly one black and one white ball.

Classically, opening one box and then the other should yield the same output as opening two boxes simultaneously. But if two boxes are opened at the same time the probability that two balls of different colors will occur is $1 - \mathbb{P}(\text{Two balls of the same color}) \leq 1 - 1/3 = 2/3$. So, if the game is played n rounds the probability of getting two balls of different color in each round is bounded by $(2/3)^n$ which converges to 0 if n goes to infinity.

This raises the question if *the balls already had a color before the boxes were opened, respectively measured*? So, if we are confronted with the situation that we always see one black and one white ball we might be convinced that the balls had no colors before the measurement was performed and that opening one of the boxes influences what is hidden behind the other two.

Another important feature of quantum mechanics which is illustrated in this example is that we never have simultaneous access to all three boxes. Classically however, we assume to have this freedom.

In the sequel we will formally introduce contextuality and we will establish a connection between the integral functions $t^\circ \in \mathcal{B}^f$ (for f defined as in (2.3)) and contextuality with respect to Pauli matrices.

The connection between contextuality and integral points in $(Q_k^f)^\circ$

Formally, we introduce (state independent) contextuality with the following definition[17]:

Definition 3.3.1. Let $\mathcal{O}$ be a set of observables (that is to say, a set of matrices). A *non-contextual value assignment* (NCVA) for $\mathcal{O}$ is a map $\lambda : \mathcal{O} \to \mathbb{C}$ such that $\lambda(O)$ is an eigenvalue of O for all $O \in \mathcal{O}$ and the map satisfies

(i) $\lambda(O_1O_2) = \lambda(O_1)\lambda(O_2)$ for all $O_1, O_2 \in \mathcal{O}$ with $O_1O_2 = O_2O_1$.

(ii) $\lambda(\omega O) = \omega\lambda(O)$ for all $\omega \in \mathbb{C}$, $O \in \mathcal{O}$, that is, λ can be linearly extended to scalar multiples of the observables.

Intuitively, this means that if one measures the observable O one gets an outcome $\lambda(O)$ that is independent of the *context* in which O is measured. A context refers to a set of commuting observables. If a set of observables does not admit an NCVA, it is called *state independent contextual*. We will always assume that the set of observables is closed under the multiplication of commuting elements (which is also necessary for λ to be well-defined).

The classical example for a set of state independent contextual observables is given in Figure 3.8. The illustration is also known as the Mermin-Peres square [18]. A simple proof that the set exhibits state independent contextuality can be found in [17, Section IV] and a proof with a topological flavor in [19].

Here, we will give an alternative proof based on another observation - essentially, we have faced this diagram several times related to integral functions $t^\circ : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ where $\text{supp}\{t^\circ\} \subset \mathbb{F}_2^{2n}$ is CAO but $t^{\circ,*} \notin (Q_k^f)^\circ$ (e.g., Figure 3.1).

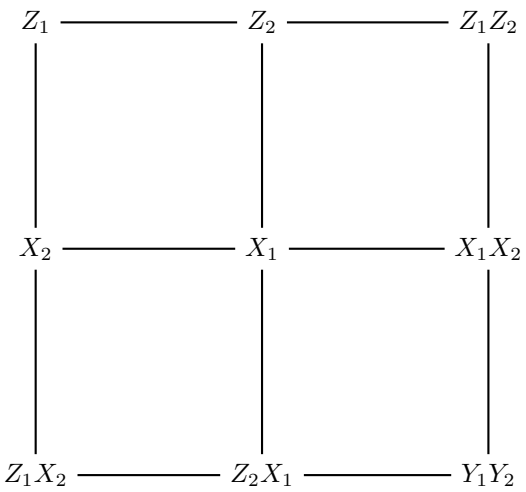

Figure 3.8: The Mermin-Peres square. Note that all rows and columns represent a single context and the matrices of each row and column multiply to I, except for the most right column which multiplies to $-I$.

From now on we concentrate on sets of Pauli observables, i.e., $\mathcal{O} \subset \mathcal{P}_n$ (and we will write $g \in \mathcal{O}$ for consistency) which are closed under the multiplication of commuting elements and under phase shifts, i.e., if $g \in \mathcal{O}$ then $\omega g \in \mathcal{O}$ for all $\omega \in \{1, -1, i, -i\}$. As a main result, we will see that the sets of Pauli observables admitting an NCVA are strongly related to integral functions in $(Q_k^f)^\circ$ for $k \geq 2$. Even more, the functions $t^\circ \in \mathcal{B}^f$ can essentially be seen as NCVAs for the set $r^{-1}(\text{supp}\{t^\circ\}) \subset \mathcal{P}_n$. Besides, for the remaining part of this thesis we assume that the function f has exactly the form of equation (2.3).

Theorem 3.3.2. *There is a bijection*

$$\{\lambda : \mathcal{O} \to \{\pm 1, \pm i\} \mid \lambda \text{ NCVA for } \mathcal{O},\, \mathcal{O} \subset \mathcal{P}_n\} \longleftrightarrow \mathcal{B}^f. \tag{3.22}$$

In other words, all possible NCVA's for sets of Pauli observables can be interpreted as integral points in the polytope $(Q_k^f)^\circ$.

Proof. Let $t^\circ \in \mathcal{B}^f$. We will construct the associated NCVA λ^{t° for the unique set of observables $\mathcal{O} \subset \mathcal{P}_n$ with $r(\mathcal{O}) = \text{supp}\{t^\circ\}$ (uniqueness follows since we assume that $\mathcal{O}$ is closed under phase shifts). For $g \in P_n$ with $r(g) \in \text{supp}\{t^\circ\}$ we set $\lambda^{t^\circ}(g) = t^\circ(r(g)) \in \{1, -1\}$. In general, we set $\lambda^{t^\circ}(g) = \chi(g) \cdot t^\circ(r(g))$ for all $g \in \mathcal{P}_n$ with $r(g) \in \text{supp}\{t^\circ\}$ guaranteeing that $\lambda^{t^\circ}(\omega g) = \omega \lambda^{t^\circ}(g)$ for all $\omega \in \{1, -1, i, -i\}$. The construction ensures that λ^{t° maps to the eigenvalues of the corresponding observable, that is $\lambda^{t^\circ}(g) \in \{1, -1\}$ if $g \in \pm P_n$ and $\lambda^{t^\circ}(g) \in \{i, -i\}$ if $g \in \pm i P_n$.

We have to show that the map λ^{t° is multiplicative. Therefore, consider commuting

$g_1, g_2 \in \mathcal{P}_n$ with $r(g_1), r(g_2) \in \mathrm{supp}\{t^\circ\}$, i.e., we have $r(g_1) \cdot r(g_2) = 0$. Since $t^\circ \in \mathcal{B}^f$, Theorem 3.2.2 implies that t° satisfies Condition (A2), that is $t^\circ(h_1 + h_2) f(h_1, h_2) = t^\circ(h_1) t^\circ(h_2)$ for orthogonal $h_1, h_2 \in \mathrm{supp}\{t^\circ\}$. We can put $f(h_1, h_2)$ on the other side compared to the actual form because $f(h_1, h_2) \in \{1, -1\}$ for orthogonal h_1, h_2. Then, using the identity given in equation (2.4) we obtain

$$\begin{aligned}
\lambda^{t^\circ}(g_1) \cdot \lambda^{t^\circ}(g_2) &= \Big(\chi(g_1) \cdot t^\circ(r(g_1))\Big) \cdot \Big(\chi(g_2) \cdot t^\circ(r(g_2))\Big) \\
&= \underbrace{\chi(g_1) \cdot \chi(g_2) \cdot f(r(g_1), r(g_2))}_{=\chi(g_1 g_2)} \cdot t^\circ(r(g_1) + r(g_2)) \\
&= \chi(g_1 g_2) \cdot t^\circ(r(g_1 g_2)) \\
&= \lambda^{t^\circ}(g_1 g_2),
\end{aligned}$$

Hence, we have proved the desired property of λ^{t°.

Conversely, let $\mathcal{O} \subset \mathcal{P}_n$ and let $\lambda : \mathcal{O} \to \mathbb{C}$ be an NCVA for $\mathcal{O}$. We will construct an integral function $t^\circ_\lambda \in \mathcal{B}^f$ for λ with $\mathrm{supp}\{t^\circ_\lambda\} = r(\mathcal{O})$. For $g \in \mathcal{O}$ with $\chi(g) = 1$ we define $t^\circ_\lambda : \mathbb{F}_2^{2n} \to \{1, -1, 0\}$ by setting $t^\circ_\lambda(r(g)) = \lambda(g)$. We want to show that $t^\circ \in \mathcal{B}^f$, which is equivalent to $t^\circ_\lambda(h_1 + h_2) = f(h_1, h_2) \cdot t^\circ_\lambda(h_1) \cdot t^\circ_\lambda(h_2)$ for all $h_1, h_2 \in \mathrm{supp}\{t^\circ_\lambda\}$ with $h_1 \cdot h_2 = 0$. Let $g_1, g_2 \in \mathcal{O}$ with $\chi(g_i) = 1$. Since

$$\begin{aligned}
t^\circ_\lambda(r(g_1)) \cdot t^\circ_\lambda(r(g_2)) = \lambda(g_1) \cdot \lambda(g_2) = \lambda(g_1 g_2) &= \chi(g_1 g_2) \cdot \lambda(\chi(g_1 g_2) \cdot g_1 g_2) \\
&= \chi(g_1 g_2) \cdot t^\circ_\lambda(r(g_1 g_2)) \\
&= f(r(g_1), r(g_2)) \cdot t^\circ_\lambda(r(g_1 g_2))
\end{aligned}$$

and $\mathrm{supp}\{t^\circ\} = r(\mathcal{O} \cap P_n)$, it follows $t^\circ \in \mathcal{B}^f$. In the last equation we once again used the identity (2.4). □

Essentially, we have shown that for every non-contextual set $\mathcal{O} \subset \mathcal{P}_n$ the map

$$\begin{aligned}
\{\lambda \text{ NCVA for } \mathcal{O}\} &\to \{t^\circ \,|\, \mathrm{supp}\{t^\circ\} = r(\mathcal{O})\} \\
\lambda &\mapsto t^\circ,
\end{aligned}$$

where

$$t^\circ(r(g)) = \begin{cases} \lambda(g), \text{ if } g \in \mathcal{P}_n,\ \chi(g) = 1, \\ 0, \text{ otherwise} \end{cases}$$

is bijective. A consequence is the following corollary:

Corollary 3.3.3. *Let $\mathcal{O} \subset \mathcal{P}_n$ be a set of Pauli observables.*

(i) If $\mathcal{O}$ admits an NCVA, it must hold $r(\mathcal{O}) \in \mathcal{K}$.

(ii) If the graph $G(r(\mathcal{O}))$ contains an induced 4-cycle, then $\mathcal{O}$ is state independent contextual.

The proof of (i) is an immediate consequence of the last theorem and the results of Section 3.2. The statement (ii) can be deduced from (i) because an induced 4-cycle in $G(r(\mathcal{O}))$ means that $r(\mathcal{O}) \notin \mathcal{K}$ by Lemma 3.2.5. The corollary can be easily applied to the Mermin-Peres square setup (Figure 3.8). If we consider the observables X_1, Z_1, X_2, Z_2, their images form a square in the commutativity graph and due to (ii) of the corollary the set of observables is state independent contextual.

In general, we want to examine how observables interact with a state ρ. This motivates the definition of a non-contextual hidden variable model[1]:

Definition 3.3.4. A *non-contextual hidden variable model* (NCHVM) for the *setup* $(\rho, \mathcal{O})$ is a triple $(\mathcal{O}, q_\rho, \mathcal{B})$ where $\mathcal{O}$ is a set of observables, $\mathcal{B}$ is a set of NCVA's for the observables $\mathcal{O}$ and q_ρ is a probability distribution over $\mathcal{B}$ related to the state ρ. Additionally, we have the property:

$$\mathrm{Tr}\,(\rho\, O) = \sum_{\lambda \in \mathcal{B}} q_\rho(\lambda) \cdot \lambda(O) \tag{3.23}$$

for all $O \in \mathcal{O}$.

If a setup $(\rho, \mathcal{O})$ does not admit an NCHVM for $(\rho, \mathcal{O})$, it is said to be *contextual*. The set $\mathcal{B}$ can always be chosen maximal - if we do not require some NCVA λ we just set $q_\rho(\lambda) = 0$.

If we focus on Pauli observables, we can rephrase the definition by Theorem 3.3.2. Let $\mathcal{O} \subset \mathcal{P}_n$ and ρ be state with polarization vector $t_\rho : \mathbb{F}_2^{2n} \to \mathbb{R}$ defined as $t_\rho(r(g)) = \mathrm{Tr}\,(\rho g)$ for $g \in P_n$. For admitting an NCVA the set of observables $\mathcal{O}$ has to satisfy $K := r(\mathcal{O}) \in \mathcal{K}$. Let $\mathcal{B}$ be the set of NCVAs for $\mathcal{O}$. Due to Theorem 3.3.2 the assignments in $\mathcal{B}$ can be encoded by elements $t^\circ \in \mathcal{B}^f$ with $\mathrm{supp}\{t^\circ\} = K$. For an NCVA λ let $t^\circ_\lambda \in \mathcal{B}^f$ with $\mathrm{supp}\{t^\circ\} = r(\mathcal{O})$ be the associated element in $\mathcal{B}^f$, i.e., $\lambda(g) = t^\circ_\lambda(r(g))$ for $g \in \mathcal{O}$ with $\chi(g) = 1$. Hence, we can rephrase Condition (3.23) as

$$t_\rho(r(g)) = \mathrm{Tr}\,(\rho g) = \sum_{\lambda \in \mathcal{B}} q_\rho(\lambda) \cdot \lambda(g) = \sum_{\lambda \in \mathcal{B}} q_\rho(\lambda) \cdot (t^\circ_\lambda)_{|K}(r(g))$$

for all $g \in \mathcal{O}$ with $\chi(g) = 1$, which is equivalent to

$$(t_\rho)_{|K} = \sum_{\lambda \in B} q_\rho(\lambda)(t^\circ_\lambda)_{|K}.$$

If we choose $\mathcal{B}$ maximal, the sum ranges over all $t^\circ \in \mathcal{B}^f$ with $\mathrm{supp}\{t^\circ\} = r(\mathcal{O})$. Now, the existence of the probability distribution q_ρ that satisfies the above equality is equivalent to $(t_\rho)_{|K}$ being a convex combination of $t^\circ_{|K}$ with $t^\circ \in \mathcal{B}^f$ with $\mathrm{supp}\{t^\circ\} = r(\mathcal{O})$. Thus, we have the characterization:

[1] There are several definitions of contextuality. For a detailed discussion see [20][21].

Lemma 3.3.5. *Let $\mathcal{O} \subset \mathcal{P}_n$ be a set of Pauli observables and ρ a state. The setup $(\rho, \mathcal{O})$ admits an NCHVM if and only if $K := r(\mathcal{O}) \in \mathcal{K}$ and $(t_\rho)_{|K^*} \in Q^K$ where*

$$Q^K = \text{conv}\{t^{\circ,*} \,|\, t^\circ \in \mathcal{B}^f(K), \text{supp}\{t^\circ\} = K\}. \tag{3.24}$$

Hence, contextuality of the setup $(\rho, \mathcal{O})$ can be interpreted as a membership problem of Q^K (given that $\mathcal{O}$ admits an NCVA). The polytope Q^K is the convex hull of the integral functions $t^{\circ,*}$ with $t^\circ : K \to \{0, 1, -1\}$ and maximal support in the polytope $(Q_k^f(K))^\circ$. In the following theorem we will see that there is an even stronger connection, more precisely, $Q_k^f(K)$ and Q^K are dual to each other if k is chosen properly.

Theorem 3.3.6. *Let $K \in \mathcal{K}$ with $K = H \cup (h_1 + H) \cup \cdots \cup (h_\ell + H)$ where H is an isotropic subspace of dimension $k-1$, $h_1, ..., h_\ell \in H^\perp$ and $h_i \cdot h_j = 1$ for all $i \neq j$. Then $Q_k^f(K)$ is a reflexive polytope and*

$$\begin{aligned} Q_k^f(K) &= \text{conv}\{t^* \,|\, t \in \mathcal{A}_k^f(K)\} \\ &= \{x : K^* \to \mathbb{R} \,|\, (t^{\circ,*})^T x \geq -1 \,|\, t^\circ \in \mathcal{B}^f(K), \text{supp}\{t^\circ\} = K\} \\ &= (Q^K)^\circ, \end{aligned}$$

where Q^K is defined as in (3.24).

"Dually" to the theorem we have

$$Q^K = \{x : K^* \to \mathbb{R} \,|\, (t^*)^T x \geq -1 \text{ for all } t \in \mathcal{A}_k^f(K)\}.$$

The proof requires some preparations. For $K \in \mathcal{K}$ and $t^\circ \in \mathcal{B}^f(K)$ we define the set

$$\begin{aligned} \mathcal{M}^{t^\circ} &= \{t^* \in \mathcal{V}(Q_k^f(K)) \,|\, (t^{\circ,*})^T t^* \neq -1\} \\ &= \{t^* \in \mathcal{V}(Q_k^f(K)) \,|\, t^\circ_{|\text{supp}\{t\}} = t_{|\text{supp}\{t\}}\}. \end{aligned}$$

Note that if $K = H \cup (h_1 + H) \cup \cdots \cup (h_\ell + H)$ we have $\mathcal{M}^{t^\circ} = \{t_1, ..., t_\ell\}$ where $\text{supp}\{t_i\} = H \cup (h_i + H)$, $(t_i)_{|H} = t^\circ_{|H}$ and $t_i(h_i) = t^\circ(h_i)$. The remaining value assignments for $h_r + h \in h_r + H$, $h \in H$ are determined by $t_i^\circ(h_r + h) = f(h_r, h) t_i^\circ(h_r) t_i^\circ(h)$.

The goal is to show that for every facet F there exists $t^\circ \in B^f(K)$ such that $(t^{\circ,*})^T t^* = -1$ for all $t^* \in \mathcal{V}(F)$. This will be the crucial observation to prove the theorem.

Lemma 3.3.7. *Let $K \in \mathcal{K}$ and $K = H \cup (h_i + H) \cup \ldots (h_\ell + H)$ where H is a $(k-1)$-dimensional isotropic subspace, $h_1, ..., h_\ell \in H^\perp$ and $h_i \cdot h_j = 1$ for all $i \neq j$. If F is a face of $Q_k^f(K)$, then there is $t^\circ \in \mathcal{B}^f(K)$ with $\text{supp}\{t^\circ\} = K$ such that $\mathcal{V}(F) \cap \mathcal{M}^{t^\circ} = \emptyset$.*

Proof. We will prove the statement by contraposition. Let $F = \text{conv}\{t^* \,|\, t^* \in \mathcal{I}\}$ where $\mathcal{I} \subset \mathcal{V}(Q_k^f(K))$ such that $\mathcal{I} \cap \mathcal{M}^{t^\circ} \neq \emptyset$ for all $t^\circ \in \mathcal{B}^f(K)$ with $\text{supp}\{t^\circ\} = K$. We will show

that $0 \in F$ and as the origin is an interior point of the polytope $Q_k^f(K)$ the set F cannot be one of its faces.

We fix $t \in \mathcal{A}_{k-1}^f(H)$ (consequently, $\operatorname{supp}\{t^\circ\} = H$, as $\dim H = k$). We encode all functions $t_a^\circ \in \mathcal{B}^f(K)$ satisfying $t_{|H} = (t_a^\circ)_{|H}$ by bitstrings $a \in \{1,-1\}^\ell$, where we set $t_a^\circ(h_i) = a_i$ (every element in the coset $h_i + h \in h_r + H$, $h \in H$ is determined by $t_a^\circ(h_i + h) = f(h_i, h) \cdot t_a^\circ(h_i) \cdot t_i^\circ(h)$). Then, $\mathcal{M}^{t_a^\circ} = \{t_1^{a,*}, ..., t_\ell^{a,*}\} \subset \mathcal{A}_k^f(K)$ with $t_i^a(h) = t(h) = t_a^\circ(h)$ for all $h \in H$ and $t_i^a(h_i) = a_i$ (and we have $\operatorname{supp}\{t_i^a\} = H \cup (h_i + H)$).

Since $\mathcal{V}(F) \cap \mathcal{M}^{t_a^\circ} \neq \emptyset$ for all $a \in \{1,-1\}^\ell$, there is at least one $r \in \{1, ..., \ell\}$ such that $t_r^{a,*} \in \mathcal{V}(F) \cap \mathcal{M}^{t_a^\circ}$. We can interpret this as follows:
Every t_a° is labeled by the associated bitstring $a = (a_1, ..., a_\ell) \in \{1,-1\}^\ell$ and every $t_i^{a,*} \in \mathcal{M}^{t_a^\circ}$ is labeled by the value $a_i \in \{1,-1\}$ for $i = 1, ..., \ell$. Now, $\mathcal{V}(F) \cap \mathcal{M}^{t_a^\circ} \neq \emptyset$ for all $a \in \{1,-1\}^\ell$ means that we have to cover each string $a \in \{1,-1\}^\ell$ by at least one value a_i for some $i \in \{1, ..., \ell\}$. If a_i covers a, we have $t_i^{a,*} \in \mathcal{V}(F) \cap \mathcal{M}^{t^\circ}$, i.e.,

$$(t_a^\circ)_{|H \cup (h_i + H)} = (t_i^a)_{|H \cup (h_i + H)}.$$

For covering all strings we require at least one position $i \in \{1, ..., \ell\}$ such that the elements labeled by $a_i = 1$ and $a_i = -1$ lie in F. That is to say, there is $i \in \{1, .., \ell\}$ and $a, \tilde{a} \in \{1,-1\}^\ell$ with $a_i = -\tilde{a}_i$ such that $t_i^{a,*}, t_i^{\tilde{a},*} \in \mathcal{V}(F) \cap (\mathcal{M}^{t_a^\circ} \cup \mathcal{M}^{t_{\tilde{a}}^\circ})$. The functions $t_r^{a,*}$ and $t_r^{\tilde{a},*}$ coincide on H^* but they differ on the coset $(h_i + H)$ since for $h_i + h \in h_i + H$ we have

$$t_r^{a,*}(h_i + h) = f(h_i, h) \cdot \underbrace{t_r^{a,*}(h_i)}_{= -t_r^{\tilde{a},*}(h_i)} \cdot \underbrace{t_r^{a,*}(h)}_{= t_r^{\tilde{a},*}(h)} = -f(h_i, h) \cdot t_r^{\tilde{a},*}(h_i) \cdot t_r^{\tilde{a},*}(h),$$

and if we consider the midpoint of the line segment $[t_r^{a,*}, t_r^{\tilde{a},*}] \subset Q_k^f(K)$, we get

$$\frac{1}{2}(t_r^{a,*} + t_r^{\tilde{a},*})(u) = \begin{cases} t(u), \text{ if } u \in H^* \\ 0, \text{ if } u \in h_i + H \\ 0, \text{ if } u \in K \setminus \{H^* \cup (h_i + H)\}. \end{cases} \tag{3.25}$$

Since $t \in \mathcal{A}_{k-1}^f(H)$ with $\operatorname{supp}\{t\} = H$ was chosen arbitrarily, we find such a tuple for all elements in $\mathcal{A}_{k-1}^f(H)$. We can label them as t_h for $h \in H$ (as $|\mathcal{A}_{k-1}^f(H)| = |H|$, due to Proposition 3.1.2 (i)) and the tuples as $t_{1,h}^*, t_{2,h}^* \in \mathcal{V}(F)$. Taking the convex combination of all these elements and evaluating it at $u \in K^*$ we get

$$\frac{1}{2|H|} \sum_{h \in H} (t_{1,h}^* + t_{2,h}^*)(u) = \begin{cases} \sum_{h \in H} t_h^\circ(u) = 0, \text{ if } u \in H^* \\ 0, \text{ otherwise,} \end{cases} \tag{3.26}$$

where we used that equation (3.25) holds for every pair $t_{1,h}^*, t_{2,h}^*$ and Proposition 3.1.2 (iii). This yields $F \ni \frac{1}{2|H|} \sum_{h \in H} (t_{1,h}^* + t_{2,h}^*) = 0$, so the origin is contained in F and as it is an interior point of $Q_k^f(K)$, the set F is not a facet of $Q_k^f(K)$. □

For the proof of the theorem we will require the notion of a *dilation* of a polytope, that is if $Q = \text{conv}\{v_1, ..., v_N\}$ and $s > 0$, then $sQ = \text{conv}\{sv_1, ..., sv_N\}$. Note that a dilation does not affect the facet structure, meaning if F is a face of Q, then sF is a face of sQ of the same dimension. Moreover, if P is full-dimensional and $x \notin P$, we can dilate P with $s > 1$ such that x lies in a facet of sP.

Proof of Theorem 3.3.6. The inclusion $Q_k^f(K) \subseteq (Q^K)^\circ$ follows directly by Theorem 3.2.2 since the elements $t^{\circ,*} \in \mathcal{B}^f(K)$ are exactly the integral functions contained in $(Q^K)^\circ$.

For the other inclusion let $x : K^* \to \mathbb{R}$ such that $x \notin Q_k^f(K)$. Since $Q_k^f(K)$ is full-dimensional, we can find $s > 1$ such that $x \in sF$ where sF is a facet of the dilation $sQ_k^f(K)$ (and F is the corresponding facet of $Q_k^f(K)$). Hence, we can write x as a convex combination of the vertices of sF, that is

$$x = \sum_{s \cdot t^* \in \mathcal{V}(sF)} \lambda_{t^*} \cdot (st^*) = s \sum_{t^* \in \mathcal{V}(F)} \lambda_{t^*} \cdot t^*$$

for $\lambda_{t^*} \geq 0$ and $\sum_{s \cdot t^* \in \mathcal{V}(sF)} \lambda_{t^*} = 1$. Applying Lemma 3.3.7 there exists $t^\circ \in \mathcal{B}^f(K)$ with $\text{supp}\{t^\circ\} = K$ such that $\mathcal{V}(F) \cap \mathcal{M}^{t^\circ} = \emptyset$, i.e., $(t^{\circ,*})^T t^* = -1$ for all $t^* \in \mathcal{V}(F)$. Thus,

$$(t^{\circ,*})^T x = s \sum_{t^* \in \mathcal{V}(F)} \lambda_{t^*} (t^{\circ,*})^T t^* = -s \sum_{t^* \in \mathcal{V}(F)} \lambda_{t^*} = -s < -1$$

implying $x \notin (Q^K)^\circ$, which finishes the proof. □

Having characterized the facets of Q^K (respectively the vertices of $(Q^K)^\circ$) we are able to deduce an interesting property of non-contextual sets of Pauli-observables, meaning they cannot be used to exhibit contextuality for a given state ρ.

Corollary 3.3.8. *If $\mathcal{O} \subset \mathcal{P}_n$ admits an NCVA, the setup $(\rho, \mathcal{O})$ does not exhibit contextuality for all states ρ, i.e., there is an NCHVM for $(\rho, \mathcal{O})$.*

Proof. Let $r(\mathcal{O}) = K = H \cup (h_1 + H) \cup \cdots \cup (h_\ell + H) \in \mathcal{K}$ where $\dim(H) = k-1$ and let A be an Hermitian matrix with $\text{Tr}\, A = 1$ and polarization vector $t_A : \mathbb{F}_2^{2n} \to \mathbb{R}$ where $t(r(g)) = \text{Tr}\,(Ag)$ for all $g \in P_n$. We will show that $(t_A)_{|K^*} \in Q^K$ is equivalent to $\text{Tr}\,(AP_S) \geq 0$ for all projectors P_S onto the $+1$ eigenspace of abelian subgroups S with $r(S) = H \cup (h_i + H)$ for some $i \in \{1, ..., \ell\}$ by using Theorem 3.3.6. Since the projectors P_S are positive semidefinite, it follows that $\text{Tr}\,(\rho P_S) \geq 0$ for all states ρ and $(t_\rho)_{|K^*} \in Q^K$ which implies that the setup $(\rho, \mathcal{O})$ admits an NCHVM.

Note that $(t_A)_{|K^*} \in Q^K$ is equivalent to $(t^*)^T (t_A)_{|K^*} \geq -1$ for all $t \in \mathcal{A}_k^f(K)$ due to Theorem 3.3.6. We define $t' \in \mathcal{A}_k^f$ by $t'(h) = t(h)$ for all $h \in \text{supp}\{t\}$ and $t(h) = 0$ otherwise,

so $\text{supp}\{t'\} = H \cup (h_i + H)$ for some $i \in \{1, ..., \ell\}$. The associated projector to t' is

$$P_S = \frac{1}{2^k} \sum_{g \in S} t'(r(g))g, \tag{3.27}$$

where $S = r^{-1}(\text{supp}\{t'\}) \cap P_n$ (the abelian subgroup associated to P_S is $\{t'(r(g)) \cdot g \,|\, g \in S\}$ in this case). Since $Q_k^f \subset Q_n^f$ (Lemma 3.1.6), we can write t' as a convex combination of elements in Q_n^f whose associated projectors have rank 1 and which are psd (these are exactly the projectors on the stabilizer states). Thus, P_S is psd as a convex combination of psd matrices. Observing that

$$\begin{aligned}
\text{Tr}\,(\rho P_S) &= \text{Tr}\left(\Big(\frac{1}{2^n} \sum_{g \in P_n} \text{Tr}\,(Ag)g\Big)\Big(\frac{1}{2^k} \sum_{g \in S} t'(r(g))g\Big)\right) \\
&= \frac{1}{2^{n+k}} \sum_{g \in S} \Big(t_A(r(g)) \cdot t'(r(g))\Big) \cdot \text{Tr}\,(g^2) \\
&= \frac{1}{2^k} \sum_{g \in S} t_A(r(g)) \cdot t'(r(g)) \\
&= \frac{1}{2^k} (t_A)^T t' \\
&= \frac{1}{2^k} ((t_A)_{|K})^T t \\
&= \frac{1}{2^k} (t(0) t_A(0) + (t^*)^T (t_A)_{|K^*}) \\
&= \frac{1}{2^k} (1 + (t^*)^T (t_A)_{|K^*})
\end{aligned}$$

we obtain that $\text{Tr}\,(AP_S) \geq 0$ iff $(t^*)^T (t_A)_{|K^*} \geq -1$. If $(t^*)^T (t_A)_{|K^*} \geq -1$ for all $t \in \mathcal{A}_k^f(K)$, then $(t_A)_{|K^*} \in Q^K$ due to Theorem 3.3.6. Now, using the fact that $\text{Tr}\,(\rho P_S) \geq 0$ for all states ρ we have $(t_\rho)_{|K^*} \in Q^K$ implying that the setup $(\rho, \mathcal{O})$ admits an NCHVM. □

Chapter 4

Conclusion and outlook

We have introduced and examined a family of integral polytopes that proved to be extremely useful to analyze the stabilizer polytope SP_n, as its linear embedding in the real Euclidean space, the polytope Q_n^f, is contained in this family. Especially, the integral points in the corresponding dual polytope turned out to be interesting and by characterizing their support we were able to establish a strong connection between SP_n and contextuality. Broadly speaking, there is a one-to-one correspondence between non-contextual value assignments for Pauli observables and integral points in Q_n^f. Additionally, the inclusion maximal sets of non-contextual Pauli observables define facets of SP_n since maximal value assignments are vertices of the dual polytope $(Q_n^f)^\circ$. By using projections of the polytope Q_n^f and proving that they are reflexive polytopes we showed that a set of Pauli observables $\mathcal{O}$ admits an NCVA then $(\rho, \mathcal{O})$ admits an NCHVM for all states ρ.

A characterization of non-contextual sets of Pauli observables has been recently done by Raussendorf et al. in [5] producing the same results and similar connections have been established for the qudit case [6] using graph based contextuality (for details see [21],[6]). In these works contextuality was identified as a resource for performing quantum computation with magic states.

There are still several open questions related to the results presented in this work - probably the most interesting one if the derived (non-)contextuality related facets of SP_n suffice to fully describe the stabilizer polytope, or, equivalently, whether Q_n^f is reflexive. We will devote a short extra subsection to another interesting family of valid inequalities for Q_n^f. In general, the stabilizer polytope appears to be an extremely interesting object whose geometric properties seem to be rather unknown. Nevertheless, a better understanding could be crucial to create a strong mathematical basis for quantum computation with magic states. As a next step one might resort to the help of software to examine SP_n, respectively Q_n^f for small numbers of n.

Besides, it might be worth to take a closer look at the graphs $G(\text{supp}\{t^\circ\})$ for $t^\circ \in \mathcal{B}^f$. We have seen that they are induced 4-cycle free and the vertex set is closed under the addition of orthogonal elements but it could be possible that they even hide more interesting combinatorial structure.

Apart from that we have constructed a mathematical new framework for the qubit stabilizer polytope, such a framework could also be fruitful to analyze the qudit case, even if this case has already been studied more extensively.

Other Facets of Q_k^f?

Apart from the inequalities arising from integral points in Q_k^f there is another, rather "set theoretic" family of valid inequalities. We will introduce them as follows: Given a set M in the phase space $\mathbb{F}_2^{2n}$ what is value

$$\max_{t\in\mathcal{A}_k^f} \sum_{h\in M} |t(h)| \,?$$

As the support of each $t \in \mathcal{A}_k^f$ is a k-dimensional isotropic subspace and $|t(h)| \in \{0, 1, -1\}$ this value coincides with maximal number of mutually orthogonal elements in M such that the dimension of their span is bounded by k.

We define the following function on the power set of $(\mathbb{F}_2^{2n})^*$:

$$\begin{aligned} s_k : 2^{(\mathbb{F}_2^{2n})^*} &\to \mathbb{N} \cup \{0\} \\ M &\mapsto \max\{|H| \,|\, H \subset H^\perp, \dim(\operatorname{span}\{H\}) = k\} \end{aligned}$$

Note that H does not have to be a subspace but just an isotropic set. For example, if we look at the set $M = \{x_1, x_2, x_3, y_3\}$ the largest isotropic subset contains 3 elements but $\dim(\operatorname{span}\{x_1, x_2, r(X_3)\}) = 3$. Hence, $s_1(M) = 1$, $s_2(M) = 2$ and $s_k(M) = 3$ for all $k \geq 3$. By definition, every $t \in \mathcal{A}_k^f$ satisfies

$$\sum_{h\in M} |t(h)| \leq s_k(M) \tag{4.1}$$

for all $M \subseteq (\mathbb{F}_2^{2n})^*$.

Even more, this inequality is satisfied by all functions $t : \mathbb{F}_2^{2n} \to \{0, 1, -1\}$ with $t(h)t(h') = 0$ if $h \cdot h' = 1$ (A1) and $|t| \leq 2^k$ (A3). This gives rise to another interesting polytope, namely the convex hull of all functions satisfying (A1) and (A3). Their properties could help to develop a better intuition for the stabilizer polytope.

The function s_k has some similarities to the rank function of a matroid, for example we have monotonicity, that is $s_k(M) \leq s_k(M')$ for all $M \subset M'$ (for more details about matroids see [8] and [22]). Yet, in contrast to rank functions of matroids s_k is not *submodular*, meaning that we can find sets $M_1, M_2 \subset (\mathbb{F}_2^{2n})^*$ such that $s_k(M_1 \cup M_2) + s_k(M_1 \cap M_2) > s_k(M_1) + s_k(M_2)$. For instance, if we take $M_1 = \{x_1, z_1\}$ and $M_2 = \{x_1x_2, z_1\}$, then $s_k(M_1) = s_k(M_2) = 1$ but $s_k(M_1 \cap M_2) + s_k(M_1 \cup M_2) = 1 + 2 > 2$ for $k \geq 2$.

Another interesting question is how the inequalities of the form (4.1) and the ones coming from the integral functions in $\mathcal{B}^f$ are related. Especially the case $k = n$ might be a worth a closer look. If the polytope Q_n^f was reflexive (which is equivalent to the statement of Question

1), these set related inequalities cannot define facets. The associated functions in $(Q_k^f)^\circ$ to inequalities as in (4.1) can be constructed as follows:
For $M \subset (\mathbb{F}_2^{2n})^*$ the inequality $\sum_{h\in M} |t(h)| \leq s_k(M)$ is equivalent to $\sum_{h\in M}(-1)^{a_h} \cdot t(h) \leq s_k(M)$ for all $a \in \{0,1\}^M$ being once again equivalent to $(x_{M,a})^T t^* \geq -1$ where the function $x_{M,a} : (\mathbb{F}_2^{2n})^* \to \mathbb{R}$ is defined via

$$x_{M,a}(h) = \begin{cases} \frac{(-1)^{a_h}}{s_k(M)}, \text{ if } h \in M \\ 0, \text{ otherwise} \end{cases}$$

and $x_{a,M} \in (Q_k^f)^\circ$. If $s_k(M) = 1$ for all $k \geq 2$, then $M = \{h_1, ..., h_\ell\} \subset (\mathbb{F}_2^{2n})^*$ and $h_i \cdot h_j = 1$ for $i \neq j$. In this case the functions $x_{M,a} : (\mathbb{F}_2^{2n})^* \to \{0, 1, -1\}$ coincide with the functions $t^\circ \in \mathcal{B}^f$ with $\text{supp}\{t^\circ\} = M$. Such a relation cannot be reproduced for sets M containing larger sets of mutually orthogonal elements.

Bibliography

[1] Peter W. Shor. Algorithms for quantum computation: Discrete logarithms and factoring. *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, 1996.

[2] Daniel Gottesman. Stabilizer codes and quantum error correction. 1997. arXiv: quant-ph/9705052v1.

[3] Daniel Gottesman. The Heisenberg Representation of Quantum Computers. 1998. arXiv: quant-ph/9807006v1.

[4] Sergei Bravyi and Alexei Kitaev. Universal quantum computation with ideal clifford gates and noisy ancillas. *Physical Review A*, 71, 2004. arXiv: quant-ph/0403025v2.

[5] Robert Raussendorf, Juani Bermejo-Vega, Emily Tyhurst, Cihan Okay, and Michael Zurel. Phase space simulation method for quantum computation with magic states on qubits. 2019. arXiv: quant-ph/1905.05374v1.

[6] Mark Howard, Joel Wallman, Victor Veitch, and Joseph Emerson. Contextuality supplies the magic for quantum computation. pages 96–96, 2015. arXiv: quant-ph/1401.4174v2.

[7] Günter Ziegler. *Lectures on Polytopes*, volume 152. 1994.

[8] Alexander Schrijver. A course in combinatorial optimization. 2003.

[9] Michael A. Nielsen and Isaac L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, New York, NY, USA, 10th edition, 2011.

[10] Jeroen Dehaene and Bart De Moor. The clifford group, stabilizer states, and linear and quadratic operations over gf(2). *Physical Review A*, 68, 04 2003. arXiv: quant-ph/0304125v1.

[11] Gabi Nebe, Eric M. Rains, and N Sloane. *Self-Dual Codes and Invariant Theory*, volume 17. 2015.

[12] Markus Heinrich and David Gross. Robustness of magic and symmetries of the stabiliser polytope, 2018. arXiv: quant-ph/1807.10296v3.

[13] Mark Howard and Earl Campbell. Application of a resource theory for magic states to fault-tolerant quantum computing. *Physical Review Letters*, 118, 2016.

[14] Audrey Terras. *Fourier Analysis on Finite Groups and Applications*. London Mathematical Society Student Texts. Cambridge University Press, 1999.

[15] David Gross. Hudson's theorem for finite-dimensional quantum systems. *Journal of Mathematical Physics*, 47:122107–122107, 2006. arXiv: quant-ph/0602001v3.

[16] Ernst Specker. Die logik nicht gleichzeitig entscheidbarer aussagen. *Dialectica*, 14:239 – 246, 05 2007.

[17] Felipe Montealegre Mora. Contextuality and the negative quasiprobability in qubit phase space, 2017.

[18] Asher Peres. Two simple proofs of the kochen-specker theorem. 1991.

[19] Cihan Okay, Sam Roberts, Stephen D. Bartlett, and Robert Raussendorf. Topological proofs of contextuality in quantum mechanics. 2017. arXiv: quant-ph/1701.01888v2.

[20] Nicolas Delfosse, Cihan Okay, Juan Bermejo-Vega, Dan E. Browne, and Robert Raussendorf. Equivalence between contextuality and negativity of the wigner function for qudits. *New Journal of Physics*, 19, 2016. arXiv: quant-ph/1610.07093v1.

[21] Adán Cabello, Simone Severini, and Andreas Winter. Graph-theoretic approach to quantum correlations. *Physical review letters*, 112:040401, 2014. arXiv: quant-ph/1401.7081v1.

[22] Michael X. Goemans. Lecture notes on matroid optimization. 2009.

Eigenständigkeitserklärung

Hiermit versichere ich, Arne Heimendahl, an Eides statt, dass ich die vorliegende Arbeit selbstständig und ohne die Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten und nicht veröffentlichten Schriften entnommen wurden, sind als solche kenntlich gemacht. Die Arbeit ist in gleicher oder ähnlicher Form oder auszugsweise im Rahmen einer anderen Prüfung noch nicht vorgelegt worden. Ich versichere, dass die eingereichte elektronische Fassung der eingereichten Druckfassung vollständig entspricht.

Köln, 5. Juni 2019