Charles University in Prague
Faculty of Mathematics and Physics
Department of Applied Mathematics

Doctoral Thesis

Jiří Fink

Probabilistic Methods in Discrete Applied Mathematics

Supervisor
Prof. RNDr. Martin Loebl, CSc.

Study program
Computer Science
Discrete Models and Algorithms

Acknowledgement

My special thanks belong to my advisor, Prof. Martin Loebl, for leading me through my doctoral studies.

I am grateful Petr Gregor, who is coauthor of the results presented in Part IV, for a great time during our joint research and numerous discussions on the topics. I would like to thank to Václav Koubek and Tomáš Dvořák for fruitful discussion and Riste Škrekovski for introducing Kreweras's conjecture to me.

Last but not least, I would like to thank all the members and the students of Department of Applied Mathematics and Institute for Theoretical Computer Science for the wonderful environment, support, and excellent background without which I would hardly write this thesis.

Hereby I declare that I have written this thesis on my own, and the references include all the sources of information I have exploited. I agree with lending of this thesis.

Prague, July 19, 2010 — Jiří Fink

Název práce:	Pravděpodobnostní metody v diskrétní aplikované matematice
Autor:	Jiří Fink
Katedra:	Katedra aplikované matematiky
Vedoucí práce:	Prof. RNDr. Martin Loebl, CSc.
E-mail vedoucího:	loebl@kam.mff.cuni.cz
Klíčová slova:	Binární lineární kódy, Teorie grafů, Edwards-Anderson Ising model, Gray kódy

Abstrakt:

Jedním ze základních problémů moderní statistické fyziky je snaha porozumět frustraci a chaosu. Základním modelem je konečně dimenzionální Edwards-Anderson Ising model. V této práci zavádíme zobecnění tohoto modelu. Studujeme množinové systémy uzavřené na symetrické rozdíly. Ukážeme, že významnou otázku, zda ground-state v Ising modelu je jednoznačný, lze studovat v těchto množinových systémech.

Krewerasova hypotéza říká, že každé perfektní párování v hyperkrychli Q_n lze rozšířit na Hamiltonovskou kružnici. Tuto hypotézu jsme dokázali.

Matching graf $\mathcal{M}(G)$ grafu G má za vrcholy perfektní párování v G a hranami jsou spojeny ty dvojice perfektních párování, jejichž sjednocení tvoří Hamiltonovskou kružnici v G. Dokážeme, že matching graf $\mathcal{M}(Q_n)$ je bipartitní a souvislý pro $n \geq 4$. Toto dokazuje Krewerasovu hypotézu, že graf M_n je souvislý, kde M_n vznikne z grafu $\mathcal{M}(Q_n)$ kontrakcí vrcholů $\mathcal{M}(Q_n)$, které odpovídají izomorfním perfektním párováním.

Cesta v Q_n vyhýbající se zadaným f chybným vrcholům se nazývá dlouhá, jestliže její délka je alespoň $2^n - 2f - 2$. Analogicky kružnice je dlouhá, pokud její délka je alespoň $2^n - 2f$. Pokud jsou všechny chybné vrcholy ze stejné bipartitní třídy Q_n, pak jsou tyto délky nejlepší možné.

Dokážeme, že pro každou množinu nejvýše $2n-4$ chybných vrcholů Q_n a každé dva bezchybné vrcholy u a v splňující jednoduchou nutnou podmínku na okolí u a v existuje dlouhá cesta mezi u a v. Počet chyb je nejlepší možný a zlepšuje předchozí známé výsledky. Také uvažujeme podstatně slabší podmínky na okolí u a v. Dokážeme, že pro každou množinu nejvýše $(n^2+n-4)/4$ chybných vrcholů Q_n existuje dlouhá cesta mezi libovolnými dvěma bezchybnými vrcholy, které mají nejvýše 3 chybné sousedy.

Označme $f(n)$ maximální číslo takové, že pro každou množinu nejvýše $f(n)$ chyb Q_n existuje dlouhá kružnice. Castañeda and Gotchev položili hypotézu, zda $f(n) = \binom{n}{2} - 2$. Nejprve jsme našli elegantní důkaz, že $f(n) \geq n^2/10 + n/2 + 1$ pro $n \geq 15$, což byl první známý kvadratický dolní odhad. Později jsme tuto hypotézu dokázali pomocí nové techniky potenciálů, kterou jsme zavedli.

Title: Probabilistic Methods in Discrete Applied Mathematics
Author: Jiří Fink
Department: Department of Applied Mathematics
Supervisor: Prof. RNDr. Martin Loebl, CSc.
Supervisor's e-mail: loebl@kam.mff.cuni.cz
Keywords: Binary linear code, Graph theory,
Edwards-Anderson Ising model, Gray codes

Abstract:

One of the basic streams of modern statistical physics is an effort to understand the frustration and chaos. The basic model to study these phenomena is the finite dimensional Edwards-Anderson Ising model. We present a generalization of this model. We study set systems which are closed under symmetric differences. We show that the important question whether a groundstate in Ising model is unique can be studied in these set systems.

Kreweras' conjecture asserts that any perfect matching of the n-dimensional hypercube Q_n can be extended to a Hamiltonian cycle. We prove this conjecture.

The *matching graph* $\mathcal{M}(G)$ of a graph G has a vertex set of all perfect matchings of G, with two vertices being adjacent whenever the union of the corresponding perfect matchings forms a Hamiltonian cycle. We prove that the matching graph $\mathcal{M}(Q_n)$ is bipartite and connected for $n \geq 4$. This proves Kreweras' conjecture that the graph M_n is connected, where M_n is obtained from $\mathcal{M}(Q_n)$ by contracting all vertices of $\mathcal{M}(Q_n)$ which correspond to isomorphic perfect matchings.

A fault-free path in Q_n with f faulty vertices is said to be *long* if it has length at least $2^n - 2f - 2$. Similarly, a fault-free cycle in Q_n is long if it has length at least $2^n - 2f$. If all faulty vertices are from the same bipartite class of Q_n, such length is the best possible.

We show that for every set of at most $2n - 4$ faulty vertices in Q_n and every two fault-free vertices u and v satisfying a simple necessary condition on neighbors of u and v, there exists a long fault-free path between u and v. This number of faulty vertices is tight and improves the previously known results. We also consider much weaker condition of neighbors of u and v. We prove that for every set of at most $(n^2 + n - 4)/4$ faulty vertices of Q_n, there exists a long fault-free path between any two vertices such that each of them has at most 3 faulty neighbors.

Let $f(n)$ be the maximum integer such that for every set of at most $f(n)$ faulty vertices of Q_n, there exists a long fault-free cycle. Castañeda and Gotchev conjectured that $f(n) = \binom{n}{2} - 2$. First, we fount an elegant proof that $f(n) \geq n^2/10 + n/2 + 1$ for $n \geq 15$ which was the first known quadratic lower bound. Later, we proved this conjecture using new technique of potentials which we introduced.

Contents

I Introduction 9

II Groundstates in Ising model 15

1 Groundstates in Ising model 17
- 1.1 Introduction . . . 17
- 1.2 Definition of a cut system . . . 18
- 1.3 Definition of a σ-XOR-system . . . 19
- 1.4 Finite XOR-systems . . . 23
- 1.5 Existence of a groundstate . . . 24
- 1.6 Distributions of weight functions ω . . . 26
- 1.7 Transitive XOR-systems . . . 31
- 1.8 Domain walls . . . 33
- 1.9 Conclusions . . . 36

III Perfect matchings 39

2 Introduction 41

3 Perfect matchings extend to H. cycles 45

4 Connectivity of matching graph 47
- 4.1 Extending with an edge . . . 47
- 4.2 Bipartiteness of $\mathcal{M}(K_{n,n})$ . . . 48
- 4.3 Walks in $\mathcal{M}(Q_d)$ . . . 49
- 4.4 Base of induction . . . 50
- 4.5 Induction step . . . 51

5 Conclusion 55

IV Long paths and cycles in faulty hypercubes 59

6 Introduction 61

7 Long path in faulty hypercube 65
- 7.1 Preliminaries . . . 65
- 7.2 Small dimension . . . 67
- 7.3 General dimension . . . 71

8 Long cycles in faulty hypercubes **75**

9 Long routing in faulty hypercubes **79**

10 Potential – overview **85**
10.1 Preliminaries 85
10.2 Overview of the proofs 86
10.3 Potentials 87

11 Paths and quadratic number of faults **89**
11.1 Induction-friendly split 89
11.2 Potentials 90

12 Cycles and optimal number of faults **97**
12.1 Induction-friendly split 97
12.2 Potentials 98

Bibliography **105**

Part I

Introduction

Binary linear codes

Discrete mathematics is a branch of mathematics which studies structures that are fundamentally discrete rather than continuous. It consists of logic, combinatorics, set theory, graph theory, probability, number theory, information theory, geometry, game theory, algebra and other various branches. Applied mathematics usually contains operations research, theoretical computer science, numerical methods, statistical mechanics, economics and many other topics.

In this thesis, we combine several of those fields to obtain results in different disciplines. A common topic is the information theory which answers fundamental questions in communication theory. It has important contributions to statistical physics, computer science, probability and statistics.

One of studied objects of the information theory is a linear code which is an important type of block code used in error correction and detection schemes. A linear code of length n and rank k is a linear subspace with dimension k of the vector space $\mathbb{F}_q^n$ where $\mathbb{F}_q$ is the finite (Galois) field with q elements. As the first class of linear codes developed for error correction purpose, famous Hamming codes have been widely used in digital communication systems.

A binary linear code is a linear code over the binary field $\mathbb{F}_2$. A vector of a binary linear code can be seen as an n-tuple of elements of the set $\{0, 1\}$, or a vertex of the n-dimensional hypercube, or as a subset of a ground set of size n. The bijection between vectors and subsets is provided by a characteristic vector of a subset. We combine those points of view depending on what is more convenient for us in particular contents.

A linear subspace of $\mathbb{F}_2^n$ corresponds to a subset of the potential set of an n element set that is closed under symmetric differences. We [38] study such set systems in Part II in connection with the Ising model which is a mathematical model of ferromagnetism in statistical mechanics.

The Ising model studies the physics of phase transitions, which arise when a small change in a parameter such as temperature or pressure causes a large and qualitative change in the state of a system. Phase transitions are common in everyday life. We can see them when water is freezing, boiling or sublimating. Another examples of phase transitions are the emergence of superconductivity in certain metals when cooled below a critical temperature, the transition between the ferromagnetic and paramagnetic phases of magnetic materials at the Curie point, and many others.

The historical interest of Ising model originally arises in study of the phenomenon of ferromagnetism which was the subject of Ising's doctoral dissertation [54] but it was invented by the physicist Wilhelm Lenz. One purpose of the Ising model is to explain how short–range interaction between molecules in a crystal give rise to long–range interaction and to predict in some sense the potential for phase transition. We study Ising model as a pure mathematical problem using combinatorics and the theory of probability.

In the model of ferromagnetism, magnetic materials are represented as lattices where vertices are atoms and edges are nearest-neighborhood interactions. Each atom has a magnetic moment which is allowed to point either "up" or "down". Magnetic moment of an atom i is called a spin, it is denoted by σ_i and its orientation is represented by $+1$ or -1. Nearest-neighborhood interactions are called coupling constants. The interaction between atoms i and j is denoted by J_{ij}. The energy of the system is called the Hamiltonian and it is defined by

$$H(\sigma) = -\sum_{\langle i,j \rangle} J_{ij}\sigma_i\sigma_j.$$

We study a state of the minimal energy which is called a groundstate.

Note that a change of a spin has influence on energy of adjacent interactions. Similarly, a change of a set of spins has influence on energy of interactions between such pairs of atoms that change a spin of exactly one atom of each pair. Furthermore, the family of all sets of interactions that can be changed by flipping some set of spins is closed under symmetric differences. In another words, this family forms a binary linear code when we consider characteristic vectors of its sets. This leads us back to our original motivation of studying the theory of information.

A binary linear code is also used in error correction which is a technique that enables reliable delivery of digital data over unreliable communication channels. In digital communication it is hard to transfer a sequence of numbers if adjacent numbers differ in more than one bit because it is very unlikely that switches will change states exactly in synchrony. In the brief period while channels are changing, the receiver will read some spurious position. In 1947, Bell Labs researcher Frank Gray [48] invented the reflected binary code which is a permutation code of numbers from 0 to 2^n-1 such that every two adjacent numbers differ in exactly one bit. Nowadays, generalizations of the reflected binary code are called Gray codes and it is used in digital communications such as digital terrestrial television and some cable TV systems.

Gray codes have found applications in such diverse areas as circuit testing [78], signal encoding [67], ordering of documents on shelves [66], data compression [77], statistics [19], graphics and image processing [2], processor allocation in the hypercube [15], hashing [31], computing the permanent [75], information storage and retrieval [14], and puzzles, a such as the Chinese Rings and Towers of Hanoi [47].

The reflected binary code has very elegant recursive construction but often more general Gray code is needed. Therefore, Gray codes having special properties are studied. An interested reader can find more details about this topic in the survey of Savage [80]. For example, is there a Gray code such that prescribed pairs of vectors that differ in a single bit are adjacent? In this point it is more convenient to switch the terminology from a Gray code to a Hamiltonian cycle in a hypercube.

Dvořák [23] showed that any set of at most $2n-3$ edges of the n-dimensional hypercube that induces vertex-disjoint paths is contained in a Hamiltonian cycle. Every Hamiltonian cycle of a hypercube can be split into 2 perfect matchings. Therefore, it is natural to ask the opposite question whether every perfect matching of the hypercube can be extended into a Hamiltonian cycle. As far as we know, the first mention of this question was published by Kreweras [59] who conjectured that answer to this question is positive. Independently, this problem was stated by Donald E. Knuth [57, problem 7.2.1.1–55]. We [35] proved this conjecture and similar results are presented in Part III.

Choosing an appropriate interconnection network is an important part of designing parallel processing or distributed systems. A large number of network topologies have been proposed [6, 89]. Among those interconnecting networks, the hypercube [7] has several excellent properties, such as a recursive structure, regularity, symmetry, small diameter, relatively short mean vertex distance, low degree, and low edge complexity which are very important when designing massively parallel or distributed systems [61].

Hamiltonian cycles and paths are used as control/data flow structures for distributed computation in arbitrary networks. An application of longest paths to a practical problem was encountered in the on-line optimization of a complex Flexible Manufacturing System [4]. These applications motivate the embedding of paths and cycles in networks. Since processor or link faults may develop in real world networks, it is important to consider faulty networks. The problems of diameter [18], routing [29], multicasting [64], broadcasting [88], gossiping [20], and embedding [32, 63] have been solved in various faulty networks.

Let $f(n)$ be the maximum integer such that $Q_n - F$ has a cycle of length at least $2^n - 2|F|$ for every set F of at most $f(n)$ vertices in n-dimensional hypercube Q_n. Firstly, Chan and Lee [13] showed that $f(n) \geq (n-1)/2$. This lower bound was improved in several papers up to $f(n) \geq 3n - 7$ by Castañeda and Gotchev [12] who conjectured that $f(n) = \binom{n}{2} - 2$. The upper bound was noticed by Koubek [58] and independently Castañeda and Gotchev [12]. We [41] obtained the first quadratic lower bound $f(n) \geq n^2/10 + n/2 + 1$, and later, we [39] proved this conjecture. These and similar results about paths in faulty hypercube are presented in Part IV.

Part II

Groundstates in Ising model

Chapter 1

Groundstates in Ising model

1.1 Introduction

A fundamental and extensively studied problem in spin glass physics is the multiplicity of infinite-volume groundstate in finite dimensinal short-ranged systems [74]. In the mean-field Sherrington-Kirkpatrick model [56], it is conjectured that finite dimensional short-ranged systems with frustration have infinitely many groundstate pairs [70, 8]. A different conjecture based on droplet-scaling theories predicts that there is only a single groundstate pair in all finite dimensions [69, 9, 42]. The later scenario has received support from recent simulations, some [1, 76] based on "chaotic size dependence" [72] and some [51] using other techniques.

Mathematically the problem remains open. Newman and Stein [73] ruled out the appearance of multiple domain walls between groundstates. Arguin et al. [3] considered the Edwards-Anderson Ising spin glass model on the half-plane $\mathbb{Z} \times \mathbb{Z}^+$. They took finite-volume measures corresponding to joint distributions of the couplings and groundstates and proved that these converge to a unique limit and the conditional distribution of the limiting measure is supported on a single groundstate pair. On the other hand, there are also papers supporting existence of different groundstate pairs [65].

We focus our attention on the nearest-neighbor Edwards-Anderson Ising model [27] on a graph $G = (V, E)$ with Hamiltonian

$$H_J(\sigma) = -\sum_{uv \in E} J_{uv}\sigma_u\sigma_v \tag{1.1}$$

where J is the set of couplings J_{uv}, $uv \in E$. We take the spins σ_u, $u \in V$, to be Ising, i.e. $\sigma_u = \pm 1$. The couplings J_{uv} are independent, identically distributed random variables and their common distribution is symmetric around zero. The most common examples are the Gaussian and $\pm J$ distribution. The Hamiltonian (1.1) has clear sense if the graph G is finite. If G is infinite, then we consider expression (1.1) as formal power series in variables J_{uv}.

In this paper, we study groundstates in an arbitrary graph and in a special class of set systems.

1.2 Definition of a cut system

For simplicity, we translate some terms of statistical physics to terms of graph theory. Instead of a state σ we consider the set of vertices $T := \{v \in V \mid \sigma(v) = -1\}$ which gives us a natural one-to-one correspondence between states and subsets of vertices. A T-*cut* is the set of edges $\mathcal{C}_T$ of G which have exactly one end-vertex in $T \subseteq V$. Note that $uv \in \mathcal{C}_T$ if and only if $\sigma_u\sigma_v = -1$ where $uv \in E$. We consider a weight function on edges $\omega : E \to \mathbb{R}$ instead of coupling constants J.

Definition 1.1. Let $G = (V, E)$ be a graph on countable many vertices V such that every vertex has finite degree and $E \neq \emptyset$. The family of all cuts of G is denoted by $\mathcal{C}_G$. The pair $(E, \mathcal{C}_G)$ is called a *cut system*.

In this paper we use the following notation.

Definition 1.2. Let $B \subseteq A$ be two sets and $\omega : A \to \mathbb{R}$ be a function. By ω_B we denote the function obtained from ω by switching the sign on elements that belong to B, that is

$$\omega_B(x) = \begin{cases} -\omega(x) & \text{if } x \in B \\ \omega(x) & \text{otherwise} \end{cases}$$

for all $x \in A$. By $\omega(B)$ we denote the sum $\sum_{x \in B} \omega(x)$.

Note that $\omega_B(B) = -\omega(B)$. The sum $\omega(B)$ is well-defined if B is finite. We use the sum $\omega(B)$ for an infinite set B only for physical motivation of the Hamiltonian but we avoid it in mathematical proofs.

Let $A, B \subseteq E$ and $S, T \subseteq V$. Let ω^T denotes $\omega_{\mathcal{C}_T}$. Observe that $(\omega_A)_B = \omega_{A \triangle B}$ where $A \triangle B = (A \setminus B) \cup (B \setminus A)$ is called the *symmetric difference of A and B*. From $\mathcal{C}_S \triangle \mathcal{C}_T = \mathcal{C}_{S \triangle T}$ it follows that $(\omega^S)^T = \omega^{S \triangle T}$. This simplifies the notation of the Hamiltonian:

$$H_J(\sigma) = -\sum_{uv \in E} J_{uv}\sigma_u\sigma_v = -\sum_{e \in E} \omega^T(e) = -\omega^T(E).$$

We are interested in a state σ (or T in the new notation) with minimal Hamiltonian. If the graph is finite we can enumerate the Hamiltonian for every state and choose the minimal one. But for a graph on infinitely many vertices, the sum $\omega^T(E)$ is not well defined. Therefore, we restrict the condition of minimality of the Hamiltonian only for finite changes: we say that T is an ω-groundstate if $-\omega^{T \triangle T'}(E) \geq -\omega^T(E)$ for every finite set $T' \subseteq V$. For a finite graph this condition already says that there is no state $T \triangle T'$ of smaller Hamiltonian. Since $\omega^{T \triangle T'}(e) = \omega^T(e)$ for every $e \in E \setminus \mathcal{C}_{T'}$, we change the last inequality to $\omega^{T \triangle T'}(\mathcal{C}_{T'}) \leq \omega^T(\mathcal{C}_{T'})$ which is well-defined even for infinite graph. Observation that $\omega^{T \triangle T'}(e) = -\omega^T(e)$ for every $e \in \mathcal{C}_{T'}$ simplifies our condition: A state $T \subseteq V$ is an ω-groundstate if $\omega^T(\mathcal{C}_{T'}) \geq 0$ for every finite set $T' \subseteq V$. For further simplification we use a definition which is a little bit stronger on some graphs.

Definition 1.3. Let $(E, \mathcal{C}_G)$ be the cut system of a graph $G = (V, E)$ and $\omega : E \to \mathbb{R}$ be a weight function. A state $T \subseteq V$ is an ω-groundstate if $\omega^T(C) \geq 0$ for every finite cut $C \in \mathcal{C}_G$.

Observe that $\mathcal{C}_T$ is finite for every finite set $T \subseteq V$ since every vertex of G has finite degree. On the other hand, it does not generally hold that $T \subseteq V$ is finite if $\mathcal{C}_T$ is finite. For example, let us consider the omnidirectional infinite path P_∞. Every finite set of edges F of P_∞ forms a cut $\mathcal{C}_T$ but the set of vertices T has to be infinite if $|F|$ is odd.

Later, we show that there always exists an ω-groundstate in more general concept. We are interested whether ω-groundstate is unique. From the observation that $\omega(e) = \omega^V(e)$ for every $e \in E$, it follows that T is an ω-groundstate if and only if $V \setminus T$ is an ω-groundstate. Such two groundstates are called *groundstate pairs* and we do not consider them as different groundstates. Note that a state $T \subseteq V$ can be also represented by a cut $\mathcal{C}_T$ which is more convenient for us because it avoids the ambiguity of groundstate pairs.

An edge $e \in E$ is *frustrated* in a state $T \subseteq V$ if $\omega^T(e) < 0$. Another problem in Edwards-Anderson Ising model is determining how large the symmetric difference of the sets of frustrated edges of two groundstates can be. Let $\mathcal{F}(\omega, T) = \left\{e \in E \;\middle|\; \omega^T(e) < 0\right\}$ be the set of frustrated edges. We show that symmetric difference of frustrated edges in two states forms a cut.

Lemma 1.4. *If $T_1, T_2 \subseteq V$ and $\omega : E \to \mathbb{R} \setminus \{0\}$, then $\mathcal{F}(\omega, T_1) \bigtriangleup \mathcal{F}(\omega, T_2) = \mathcal{C}_{T_1 \bigtriangleup T_2}$.*

Proof. An edge e belongs to $\mathcal{C}_{T_1 \bigtriangleup T_2}$ if and only if e belongs to exactly one cut of $\mathcal{C}_{T_1}$ and $\mathcal{C}_{T_2}$ which means that $\omega^{T_1}(e)$ and $\omega^{T_2}(e)$ have different signs. □

If ω is chosen randomly from the Gaussian distribution, then an edge of weight 0 occurs with probability 0.

1.3 Definition of a σ-XOR-system

We generalize our definition of a groundstate of graphs into a special type of set systems. Let us note that every cut system is closed under symmetric difference; and this property is crucial for us.

Definition 1.5. Let M be a countable set and S be a family of subsets of M such that both M and S are nonempty and $\bigcup_{A \in S} A = M$. We say that (M, S) is a *XOR-system*, if $A \bigtriangleup B \in S$ for every $A, B \in S$. Let S_k be the family of finite sets of S.

The set systems (M, S), where M or S is the empty set, are not interesting for us. If some element $m \in M$ does not occur in any set of S, then we can remove m from M, so we require that $\bigcup_{A \in S} A = M$. Note that the cut system of every graph with at least one edge forms a XOR-system.

Let us observe that S_k is countable. Indeed, S_k is countable for the complete XOR-system $(\mathbb{N}, S)$ where $S = 2^{\mathbb{N}}$. That is because S_k is countable union of countable sets R_n where R_n the set all subsets of $\mathbb{N}$ of size n; and R_n is countable because there exists an injection from R_n to the Cartesian product $\mathbb{N}^n$ which is countable.

One may ask why we require only the symmetric difference of finitely many sets in the definition of a XOR-system. That is because it is not obvious what the symmetric difference of countably many subsets of M is. First, we need to define the limit of a sequence of sets.

Definition 1.6. Let $(A_n)_{n\in\mathbb{N}}$ be a sequence of subsets of a set M. The sequence $(A_n)_{n\in\mathbb{N}}$ converges to $A \subseteq M$ if for every $m \in M$ the number of $n \in \mathbb{N}$ satisfying $m \in A \triangle A_n$ is finite. This is denoted by $\lim_{n\to\infty} A_n = A$ or $A_n \xrightarrow{n} A$.

Note that a sequence $(A_n)_{n\in\mathbb{N}}$ of subsets of a set M converges to $A \subseteq M$ if and only if for every finite set $B \subseteq M$ there exists $n_0 \in \mathbb{N}$ such that for every $n \geq n_0$ it holds that $(A_n \triangle A) \cap B = \emptyset$. We say that $x \in M$ is an *alternating item* for the sequence $(A_n)_{n\in\mathbb{N}}$ if both sets $\{n \mid x \in A_n\}$ and $\{n \mid x \notin A_n\}$ are infinite. Clearly, the sequence $(A_n)_{n\in\mathbb{N}}$ converges if and only if it has no alternating item.

Now, we define the symmetric difference of an infinite sequence $(A_n)_{n\in\mathbb{N}}$ as limit of partial symmetric differences $\triangle_{i=1}^n A_i$.

Definition 1.7. Let $(A_n)_{n\in\mathbb{N}}$ be a sequence of subsets of a set M and $B_n = \triangle_{i=1}^n A_i$ for $n \in \mathbb{N}$. The symmetric difference of the sequence $(A_n)_{n\in\mathbb{N}}$ converges to A if $B_n \xrightarrow{n} A$. This is denoted by $\triangle_{n\in\mathbb{N}} A_n = A$.

As usual, every sequence has at most one limit and at most one symmetric difference. Our main tool is compactness on a XOR-system (M, S), which states that every sequence $(A_n)_{n\in\mathbb{N}}$ of S has a subsequence $(A_{k_n})_{n\in\mathbb{N}}$ converging to $A \subseteq M$. We need to know whether the limit of a sequence of S remains in S which is provided by the following definition.

Definition 1.8. We say that a XOR-system (M, S) is closed under limits if the family S contains the limit of every converging sequence of S. We say that a XOR-system (M, S) is closed under symmetric differences if for every sequence $(A_n)_{n\in\mathbb{N}}$ of S such that $\triangle_{n\in\mathbb{N}} A_n = A$, the family S contains A.

Now, we show that it suffices to consider only the closure under limits.

Proposition 1.9. *A XOR-system (M, S) is closed under limits if and only if it is closed under symmetric differences.*

Proof. If the XOR-system (M, S) is closed under limits, then it contains limits of convergent partial symmetric differences of sequences. On the other hand, let $(A_n)_{n\in\mathbb{N}}$ be a sequence of S converging to A. Let $B_1 = A_1$ and $B_n = A_n \triangle A_{n-1}$ for $n \geq 2$. From $\triangle_{i=1}^n B_i = A_n$ it follows that $\triangle_{n\in\mathbb{N}} B_n = A \in S$. □

We use limits of sequences instead of their symmetric differences because it is more convenient for us.

Definition 1.10. If a XOR-system (M, S) is closed under limits, then we define S_σ be the set of all limits of converging sequences of S_k. A XOR-system (M, S) is called σ-XOR-system if it is closed under limits and $S = S_\sigma$.

In another words, a XOR-system (M, S) is a σ-XOR-system if S contains a limit of every converging sequence of S and for every set $A \in S$ there exists a sequence of S_k converging to A.

For example, a complete system $(M, 2^M)$ is σ-XOR-system. On the other hand, $\left(\mathbb{N}, \binom{\mathbb{N}}{even}\right)$ is not σ-XOR-system where $\binom{\mathbb{N}}{even}$ is the family of all subset of even size because the limit of the sequence $(\{1, n+1\})_{n\in\mathbb{N}}$ is $\{1\} \notin \binom{\mathbb{N}}{even}$. Later, we present examples of XOR-systems which are closed under limits but does not satisfy $S = S_\sigma$.

Let us show properties and relations between S_k and S_σ.

Lemma 1.11. *Let (M,S) be a XOR-system which is closed under limits. It holds that $S_k \subseteq S_\sigma$ and $S_k = (S_\sigma)_k$.*

Proof. If $A \in S_k$, then the constant sequence $(A)_{n\in\mathbb{N}}$ converges to A which implies that $A \in S_\sigma$ and the first part of the statement holds.

If $A \in S_k$, then $A \in S_\sigma$ which also implies that $A \in (S_\sigma)_k$. It remains to prove that $S_k \supseteq (S_\sigma)_k$.

Let $A \in (S_\sigma)_k$ which means that $A \in S_\sigma$ and A is finite. Since $S_\sigma \subseteq S$, we have $A \in S_k$. □

We say that a XOR-system (M,S) is finite if M is finite; otherwise, it is infinite. Now, we prove that every finite XOR-system is σ-XOR-system. In Section 1.4 we present more details about the boundary between finite and infinite XOR-systems.

Proposition 1.12. *Let (M,S) be a finite XOR-system. Then, (M,S) is a σ-XOR-system and $S = S_k = S_\sigma$ and they are finite.*

Proof. Since all sets of S are finite, we know that $S = S_k$. Moreover, S is finite because $|S| \le 2^{|M|}$.

Let $(A_n)_{n\in\mathbb{N}}$ be a converging sequence of S. If $(A_n)_{n\in\mathbb{N}}$ contains two different sets $A, B \in S$ infinitely many times, then every element of $A \triangle B$ is alternating, which contracts convergency of $(A_n)_{n\in\mathbb{N}}$. So, $(A_n)_{n\in\mathbb{N}}$ has only one set A infinitely many times which implies that $A_n \to A$. This proves that (M,S) is closed under limits.

Finally, $S_k \subseteq S_\sigma \subseteq S$ by definition and Lemma 1.11 which concludes the proof since $S = S_k$. □

Now, we prove that every converging sequence of S_σ has its limit in S_σ. It implies that a XOR-system (M,S) is σ-XOR-system if S contains a limit of every converging sequence of S_k and for every set $A \in S$ there exists a sequence of S_k converging to A.

Lemma 1.13. *Let (M,S) be a XOR-system which is closed under limits. For every sequence $(A_n)_{n\in\mathbb{N}}$ of S_σ converging to $A \in S$ there exists a sequence $(B_n)_{n\in\mathbb{N}}$ of S_k converging to A.*

Proof. If M is finite, then $S = S_\sigma = S_k$ by Proposition 1.12, and the statement holds. So, we assume that M is infinite and $(d_n)_{n\in\mathbb{N}}$ is a sequence of all elements of M. Let M_n be $\{d_1,\dots,d_n\}$ for every $n \in \mathbb{N}$.

Let $(A_n)_{n\in\mathbb{N}}$ be a sequence of S_σ such that $A_n \xrightarrow{n} A \in S$.

Since $A_n \in S_\sigma$, there exists a sequence $(A_n^k)_{k\in\mathbb{N}}$ of S_k such that $A_n^k \xrightarrow{k} A_n$.

Since $A_n \xrightarrow{n} A$, there exists i_m such that $(A_{i_m} \triangle A) \cap M_m = \emptyset$ for every $m \in \mathbb{N}$.

Since $A_{i_m}^k \xrightarrow{k} A_{i_m}$, there exists j_m such that $(A_{i_m}^{j_m} \triangle A_{i_m}) \cap M_m = \emptyset$ for every $m \in \mathbb{N}$.

We prove that $B_n = A_{i_n}^{j_n}$ is the requested sequence which satisfies $B_n \xrightarrow{n} A$, that is for every $m \in \mathbb{N}$ there exists $n' \in \mathbb{N}$ such that for every $n \ge n'$ it holds that $(B_n \triangle A) \cap M_m = \emptyset$. For given $m \in \mathbb{N}$ we choose $n' = m$. Let $n \ge m$. From $M_m \subseteq M_n$ it follows that

$$\begin{aligned}(B_n \triangle A) \cap M_m \subseteq (B_n \triangle A) \cap M_n = (A_{i_n}^{j_n} \triangle A) \cap M_n = \\ ((A_{i_n}^{j_n} \triangle A_{i_n}) \triangle (A_{i_n} \triangle A)) \cap M_n \subseteq ((A_{i_n}^{j_n} \triangle A_{i_n}) \cap M_n) \cup ((A_{i_n} \triangle A) \cap M_n)\end{aligned}$$

By definition of the sequence $(i_n)_{n\in\mathbb{N}}$ it holds that $(A_{i_n} \triangle A) \cap M_n = \emptyset$.
By definition of the sequence $(j_n)_{n\in\mathbb{N}}$ it holds that $(A_{i_n}^{j_n} \triangle A_{i_n}) \cap M_n = \emptyset$.
Therefore, $(B_n \triangle A) \cap M_m = \emptyset$. □

Now, we study the condition that σ-XOR-system has to be closed under limits. Later, we define a groundstate in a XOR-system and prove that (M, S) has always a groundstate and show that it suffices to study groundstates in S_σ.

If a XOR-system (M, S) is closed under limits and $S = S_\sigma$, then $(M, S) = (M, S_\sigma)$ is a σ-XOR-system. But we prove that (M, S_σ) is a σ-XOR-system even if $S_\sigma \neq S$.

Proposition 1.14. *If (M, S) is a XOR-system which is closed under limits and $\bigcup_{A \in S_\sigma} = M$, then (M, S_σ) is a σ-XOR-system.*

Proof. First, we prove that (M, S_σ) is a XOR-system. From $\emptyset \in S$ it follows that $\emptyset \in S_\sigma$. For $A, B \in S_\sigma$ there exist sequences A_n and B_n of S_k such that $A_n \xrightarrow{n} A$ and $B_n \xrightarrow{n} B$. It follows from $A_n \triangle B_n \xrightarrow{n} A \triangle B$ that $A \triangle B \in S_\sigma$, and therefore (M, S_σ) is a XOR-system.

Let $(A_n)_{n\in\mathbb{N}}$ be a sequence of S_σ converging to A. By Lemma 1.13 there exists a sequence $(B_n)_{n\in\mathbb{N}}$ of S_k converging to A. Since (M, S) is closed under limits, A belongs to S_σ. Therefore, (M, S_σ) is closed under limits too.

Clearly, $(S_\sigma)_\sigma \subseteq S_\sigma$ by definition. On the other hand, let $(A_n)_{n\in\mathbb{N}}$ be a sequence of $(S_\sigma)_k$ converging to $A \in (S_\sigma)_\sigma$. By Lemma 1.11 we know that $(A_n)_{n\in\mathbb{N}}$ is a sequence of S_k and therefore, $A \in S_\sigma$. All together, $(S_\sigma)_\sigma = S_\sigma$. □

Now, we prove that the cut system $(E, \mathcal{C}_G)$ of a graph $G = (V, E)$ forms a σ-XOR-system. Recall that we consider only graphs on countably many vertices with finite degree of every vertex.

Theorem 1.15. *If $G = (V, E)$ is a connected graph with at least one edge, then $(E, \mathcal{C}_G)$ is a XOR-system which is close under limits. Moreover, if the maximum degree of G is finite, then $(E, \mathcal{C}_G)$ is a σ-XOR-system.*

Proof. From $\mathcal{C}_\emptyset = \emptyset$ and $\mathcal{C}_{T_1} \triangle \mathcal{C}_{T_2} = \mathcal{C}_{T_1 \triangle T_2}$, it follows that $(E, \mathcal{C}_G)$ is a XOR-system.

Now, we prove that $\mathcal{C}_G$ is closed under limits. Let $(C_n = \mathcal{C}_{T_n})_{n\in\mathbb{N}}$ be a sequence of cuts of G such that $C_n \xrightarrow{n} C \subseteq E$. We prove that C is a cut of G. Let x be a vertex of G. We suppose that $x \notin T_n$; otherwise, we may consider $V \setminus T_n$ instead of T_n because $\mathcal{C}_{T_n} = \mathcal{C}_{V \setminus T_n}$.

Does the sequence $(T_n)_{n\in\mathbb{N}}$ of a subsets of V converge? If it does not, then $(T_n)_{n\in\mathbb{N}}$ contains an alternating item $u \in V$. Note that $x \neq u$. Let us consider a path from x to u and let v be the first alternating vertex in $(T_n)_{n\in\mathbb{N}}$ on that path and w be the previous vertex which is not alternating. Hence, vw is an alternating edge on $(C_n)_{n\in\mathbb{N}}$ but $(C_n)_{n\in\mathbb{N}}$ is convergent which is a contradiction. Therefore, $T_n \xrightarrow{n} T \subseteq V \setminus \{x\}$.

If $\mathcal{C}_T$ and C are different, then cut sequences $(\mathcal{C}_{T_n})_{n\in\mathbb{N}}$ and $(C_n)_{n\in\mathbb{N}}$ are different for sufficiently large n which contradicts the assumption that $\mathcal{C}_{T_n} = C_n$ for all $n \in \mathbb{N}$. Hence, $C = \mathcal{C}_T \in \mathcal{C}_G$ and $\mathcal{C}_G$ is closed under limits.

Finally, we prove that for every $\mathcal{C}_T = C \in \mathcal{C}_G$ there exists a sequence $(C_n)_{n\in\mathbb{N}}$ of finite cuts of G converging to C. If T is finite, then $\mathcal{C}_T$ is finite and we consider the constant sequence $(\mathcal{C}_T)_{n\in\mathbb{N}}$. Otherwise, let $(v_n)_{n\in\mathbb{N}}$ be a sequence of all vertices of T. Clearly, the sequence $\left(\mathcal{C}_{\{v_1,\ldots,v_n\}}\right)_{n\in\mathbb{N}}$ converges to $\mathcal{C}_T$ and $\mathcal{C}_{\{v_1,\ldots,v_n\}}$ is finite for every $n \in \mathbb{N}$. □

It is obvious that common lattices satisfy all conditions of the last theorem. On the other hand, the request that the maximum degree of G is finite, is necessary. Let $K_\mathbb{N}$ be the complete graph with infinitely countably many vertices.

Proposition 1.16. *The only finite cut of $K_{\mathbb{N}}$ is the empty one. Moreover, $(\mathcal{C}_{K_{\mathbb{N}}})_\sigma = \{\emptyset\}$.*

Proof. For a contradiction, let us suppose that there exists a finite cut $\mathcal{C}_T$ containing edge uv. Assume that $u \in T$ and $v \notin T$. For every vertex $x \in V \setminus \{u, v\}$, either xu or xv belongs into $\mathcal{C}_T$ and we denote it by e_x. Clearly, edges $\{e_x \mid x \in V \setminus \{u, v\}\}$, are pairwise different. Hence, we have infinitely many edges in $\mathcal{C}_T$ which is a contradiction.

The only sequence of finite cuts of $K_{\mathbb{N}}$ is $(\emptyset)_{n\in\mathbb{N}}$ which implies that $(\mathcal{C}_{K_{\mathbb{N}}})_\sigma = \{\emptyset\}$. □

1.4 Finite XOR-systems

One of the main tools in this article is compactness which guarantees that every sequence has a convergent subsequence. Recall that a sequence $(A_n)_{n\in\mathbb{N}}$ of subsets of a set M converges to $A \subseteq M$ if for every $m \in M$ the number of $n \in \mathbb{N}$ satisfying $m \in A \triangle A_n$ is finite. A sequence $(A_{k_n})_{n\in\mathbb{N}}$ is called a *subsequence* of a sequence $(A_n)_{n\in\mathbb{N}}$ if $(k_n)_{n\in\mathbb{N}}$ is an increasing sequence of $\mathbb{N}$.

Theorem 1.17 (Compactness)**.** *Every sequence of subsets of a set has a converging subsequence.*

The proof of this theorem follows from well know Tychonoff Theorem [84]. It holds for every set of arbitrary cardinality; nevertheless, we use it only for countable sets in this article.

A XOR-system (M, S) is finite if M is finite. Proposition 1.12 states that a finite XOR-system (M, S) satisfies $S = S_k = S_\sigma$. Such property is not expected in infinite XOR-system. But it does not hold generally that $S_k \neq S_\sigma$ if M is infinite; for example, Proposition 1.16 shows an example of XOR-system (M, S) where M is infinite but $S_\sigma = S_k = \{\emptyset\}$. We need to require that (M, S) is σ-XOR-system.

Proposition 1.18. *Let (M, S) be a σ-XOR-system. For every $m \in M$ there exists $A \in S_k$ such that $m \in A$.*

Proof. The definition of a XOR-system requires that $\bigcup_{A\in S} A = M$ which implies that there exists $A \in S$ such that $m \in A$. The definition of σ-XOR-system requires that $S = S_\sigma$ which implies that $A \in S_\sigma$. Hence, there exists a sequence $(A_n)_{n\in\mathbb{N}}$ of S_k converging to A which implies that $m \in A_n$ for sufficiently large n. □

Theorem 1.19. *Let (M, S) be a σ-XOR-system. The following statements are equivalent.*

1. *M is infinite.*
2. *S_k is infinite.*
3. *S_σ is not countable.*
4. *$S_k \neq S_\sigma$.*
5. *There exists a sequence $(A_n)_{n\in\mathbb{N}}$ of S_k such that $\bigcup_{n\in\mathbb{N}} A_n$ is infinite.*
6. *There exists a sequence $(B_n)_{n\in\mathbb{N}}$ of S_k of pair-wise disjoint nonempty sets.*

Proof. First, we prove that the statements (1), (2) and (5) are equivalent. The statement (5) implies (2) because $\bigcup_{n\in\mathbb{N}} A_n$ is not infinite if S_k is finite. From Proposition 1.12 it follows that (2) implies (1). Let $(m_n)_{n\in\mathbb{N}}$ be a sequence of all elements of M. By Proposition 1.18 there exists $A_n \in S_k$ such that $m_n \in A_n$ for every $n \in \mathbb{N}$. Therefore, $M = \bigcup_{n\in\mathbb{N}} A_n$ is infinite and (1) impies (5).

Now, we prove that (3), (4), (5) and (6) are equivalent. Since S_k is always countable, (3) implies (4).

From (4) it follows that there exists a sequence $(A_n)_{n\in\mathbb{N}}$ of S_k converging to $A \in S_\sigma \setminus S_k$. Therefore, A is infinite and $\bigcup_{n\in\mathbb{N}} A_n \supseteq A$ is also infinite which implies (5).

Now, we prove that (5) implies (6). Let $(A_n)_{n\in\mathbb{N}}$ be a sequence of S_k such that $\bigcup_{n\in\mathbb{N}} A_n$ is infinite. Note that the sequence $(A_n)_{n\in\mathbb{N}}$ has infinitely many different sets. Suppose that sets $(A_n)_{n\in\mathbb{N}}$ are pair-wise different nonempty sets, since we may consider only the first occurrence of each set in the sequence. By compactness, the sequence $(A_n)_{n\in\mathbb{N}}$ has a subsequence $(A_{k_n})_{n\in\mathbb{N}}$ converging to a set $A \in S_\sigma$.

We define B_n by induction on n. Let $B_1 = A_{k_1}$. Assume that $B_1, \dots, B_{n-1} \in S_k$ are pair-wise disjoint nonempty sets. Our aim is to find $B_n \in S_k$ such that $B_n \cap B = \emptyset$, where $B = \bigcup_{i=1}^{n-1} B_i$. Since $A_{k_n} \xrightarrow{n} A$, there exists m such that $(A_{k_{m'}} \triangle A) \cap B = \emptyset$ holds for all $m' \geq m$. Therefore,

$$(A_{k_m} \triangle A_{k_{m+1}}) \cap B = ((A_{k_m} \triangle A) \triangle (A_{k_{m+1}} \triangle A)) \cap B \subseteq \\ ((A_{k_m} \triangle A) \cap B) \cup ((A_{k_{m+1}} \triangle A) \cap B) = \emptyset.$$

Hence, we define $B_n = A_{k_{m+1}} \triangle A_{k_m}$, which is non-empty and disjoint with all sets $B_1, \dots, B_{n-1}$. This proves (6).

Let $(M_n)_{n\in\mathbb{N}}$ be a sequence of pair-wise disjoint nonempty sets by (6). For a sequence $(a_n)_{n\in\mathbb{N}}$ of $\{0,1\}$ we define a set $Z(a_n)$ to be the symmetric difference of all B_n where $a_n = 1$. For different sequences $(a_n)_{n\in\mathbb{N}}$ we obtain different sets $Z(a_n) \in S_\sigma$. The system S_σ is uncountable because there are uncountably many sequences $(a_n)_{n\in\mathbb{N}}$ which implies (3). □

Proposition 1.18 and Theorem 1.19 give us basic characterization of finite and infinite σ-XOR-systems. They also say that S_σ is either finite or uncountable for every σ-XOR-system (M, S).

1.5 Existence of a groundstate

In this section, we define a groundstate for a XOR-system and we prove that every σ-XOR-system has a groundstate. One can check that the following definition only extends the definition for cut systems into a general XOR-system.

Definition 1.20. Let (M, S) be a XOR-system and $\omega : M \to \mathbb{R}$ be a weight function. Then, $A \in S$ is an ω-groundstate if $\omega_A(B) \geq 0$ for every $B \in S_k$.

Before we study groundstates, we need two simple lemmas. The first one directly follows from the fact that $(\omega_A)_B = \omega_{A \triangle B}$.

Lemma 1.21. *Let (M, S) be a XOR-system, $A, B \in S$ and $\omega : M \to \mathbb{R}$. Then, B is an ω_A-groundstate if and only if $A \triangle B$ is an ω-groundstate.*

Lemma 1.22. *Let A and B be finite subsets of a set M and $\omega : M \to \mathbb{R}$ be a weight function. Then, $\omega_A(B \triangle A) = \omega(B) - \omega(A)$.*

Proof.

$$\begin{aligned}\omega_A(B \triangle A) &= \omega_A((B \setminus A) \cup (A \setminus B)) \\ &= \omega_A(B \setminus A) + \omega_A(A \setminus B) \\ &= \omega(B \setminus A) - \omega(A \setminus B) \\ &= (\omega(B \setminus A) + \omega(B \cap A)) - (\omega(A \setminus B) + \omega(B \cap A)) \\ &= \omega(B) - \omega(A).\end{aligned}$$

□

We prove that there always exists a groundstate in a σ-XOR-system. But we need to start with a groundstate in a finite XOR-system.

Lemma 1.23. *Every finite XOR-system (M, S) has an ω-groundstate for every $\omega : M \to \mathbb{R}$.*

Proof. Since S is finite by Proposition 1.12, we choose $A \in S$ such that $\omega(A)$ is minimal. Then, A is an ω-groundstate because $\omega_A(B) = \omega(A \triangle B) - \omega(A) \geq 0$ for every $B \in S_k$ by Lemma 1.22. □

A closure of a finite set $Z \subseteq S$ in a XOR-system (M, S) is the minimal subset of S containing Z that is closed under finite symmetric differences. Note that $(\bar{M}, \bar{Z})$ is a XOR-system where $\bar{M} = \bigcup_{A \in \bar{Z}} A$.

Theorem 1.24. *Let (M, S) be a XOR-system that is closed under limits. Then, (M, S) contains an ω-groundstate in S_σ for every $\omega : M \to \mathbb{R}$.*

Proof. Since S_k is countable there exists a sequence $(X_n)_{n \in \mathbb{N}}$ of all sets of S_k. Let $Z_n = \overline{\{X_1, \ldots, X_n\}}$. Let set A_n be an ω-groundstate of the finite XOR-system $(\bigcup_{D \in Z_n} D, Z_n)$. By compactness (Theorem 1.17) there exists a subsequence $(A_{k_n})_{n \in \mathbb{N}}$ of $(A_n)_{n \in \mathbb{N}}$ converging to $A \in S_\sigma$. We show that A is an ω-groundstate of (M, S).

For a contradiction, let $X_l \in S_k$ such that $\omega_A(X_l) < 0$. Since $A_{k_n} \xrightarrow{n} A$, there exists $n \in \mathbb{N}$ such that $k_n \geq l$ and $(A_{k_n} \triangle A) \cap X_l = \emptyset$. Hence, $X_l \in Z_{k_n}$ and $\omega_{A_{k_n}}(X_l) = \omega_A(X_l) < 0$ but A_{k_n} is an ω-groundstate in $(\bigcup_{D \in Z_{k_n}} D, Z_{k_n})$ which is a contradiction. □

The condition that XOR-system (M, S) is closed under limits is necessary. For example, let S be the set of all finite subsets of an infinite set M. Then, (M, S) is a XOR-system which is not closed under limits. If $\omega : M \to \{-1\}$, then there is no ω-groundstate because for every $A \in S$ we choose a finite and nonempty $B \subseteq M \setminus A$ to have $\omega_A(B) = \omega(B) = -|B| < 0$.

Let (M, S) be a XOR-system which is closed under limits. Let σ be the relation on S such that $A \sigma B$ if $A \triangle B \in S_\sigma$, where $A, B \in S$. The relation σ is an equivalence on S. Let us consider classes of equivalence S/σ. One of the classes of S/σ is S_σ.

One of the crucial properties of every XOR-system is called *invariance*, that is $S = \{B \triangle A \mid B \in S\}$ for every $A \in S$. From the invariance it follows that it is really easy to find an ω-groundstate in every class S/σ.

Corollary 1.25. *Every XOR-system (M, S), that is closed under limits, contains an ω-groundstate in every class of S/σ for every $\omega : M \to \mathbb{R}$.*

Proof. Let S' be a class of S/σ and $X \in S'$. By Theorem 1.24 there exists an ω_X-groundstate A in S_σ. By Lemma 1.21, $A \triangle X$ is an ω-groundstate. □

For example, let

$$\begin{aligned} S = &\{A \subset \mathbb{N} \mid |A \cap \{2n-1, 2n\}| \text{ is even } \forall n \in \mathbb{N}\} \\ &\cup \{A \subset \mathbb{N} \mid |A \cap \{2n-1, 2n\}| \text{ is odd } \forall n \in \mathbb{N}\}. \end{aligned}$$

Clearly, $(\mathbb{N}, S)$ is a XOR-system which is closed under limits and S/σ has two classes.

Let us consider the complete graph $K_{\mathbb{N}}$ on countably many vertices. By Proposition 1.16 we know that $S_\sigma = \{\emptyset\}$ which implies that every set of $\mathcal{C}_{K_{\mathbb{N}}}$ forms a class of $\mathcal{C}_{K_{\mathbb{N}}}/\sigma$. Since there are uncountably many cuts in $K_{\mathbb{N}}$, there are also uncountably many classes in $\mathcal{C}_{K_{\mathbb{N}}}/\sigma$.

Now, we know how groundstates behave between different classes in S/σ. By Corollary 1.25 we can consider only one class of S/σ; and by invariance groundstates have the same behaviour in every class S/σ. Moreover, by Theorem 1.15 common lattices satisfies $S = S_\sigma$ so we restrict our attention on σ-XOR-systems.

The following proposition proves that the limit of converging sequences of groundstates is also a groundstate.

Proposition 1.26. *Let (M, S) be a XOR-system and $\omega : M \to \mathbb{R}$ be a weight function. Let $(A_n)_{n\in\mathbb{N}}$ be a sequence of S such that A_n is an ω-groundstate for every $n \in \mathbb{N}$. If $A_n \xrightarrow{n} A$, then A is an ω-groundstate.*

Proof. Let $B \in S_k$. Since $A_n \to A$ there exists n such that $(A \triangle A_n) \cap B = \emptyset$. Hence $\omega_A(B) = \omega_{A_n}(B) \geq 0$ which proves that A is an ω-groundstate. □

1.6 Distributions of weight functions ω

As we mention in the beginning, the most common distributions for coupling constants J (or, weight function ω) are the Gaussian and $\pm J$ distributions. It is natural to consider that distribution of weight function ω is symmetric around zero.

The Hadamard product of vectors $u, v \in \mathbb{R}^M$ is the vector $u * v$ of $\mathbb{R}^M$ where $(u * v)_i := u_i v_i$ for all $i \in M$. Moreover, $u * B := \{u * x \mid x \in B\}$ where $B \subseteq \mathbb{R}^M$.

Definition 1.27. Let M be a countable set. The probability space $(\mathbb{R}^M, \mathbb{B}^M, \mathrm{P})$ is symmetric if $\mathrm{P}(B) = \mathrm{P}(s * B)$ for every $B \in \mathbb{B}^M$ and $s \in \{\pm 1\}^M$.

In $\pm J$ distribution the coupling constants are independently and uniformly chosen between two numbers $+1$ and -1. Crucial but physically unnatural property of this distribution is that it too often happens that a finite change F of a state A does not change the weight of the state A, i.e. $\omega_A(F) = 0$.

For example, let S be a family of all subsets of $\mathbb{N}$ that contains $2n$ if and only if it contains $2n-1$ for every $n \in \mathbb{N}$. Note that $(\mathbb{N}, S)$ is a σ-XOR-system which is generated by $\{\{2n-1, 2n\} \mid n \in \mathbb{N}\}$. We consider a random weight function $\omega : \mathbb{N} \to \{\pm 1\}$ with independent and uniform distribution. Let

$$I_\omega := \{n \in \mathbb{N} \mid \omega(2n-1) = -\omega(2n)\}.$$

Since the probability that $\omega(2n-1)$ and $\omega(2n)$ have the opposite sign is $\frac{1}{2}$, the set I_ω is infinite for almost every ω. Let A be an ω-groundstate. Since $I_\omega = I_{\omega_C}$ for every $C \in S$ we know that $I_\omega = I_{\omega_A}$. Observe that $B := A \triangle \{2n-1, 2n \mid n \in Z\}$ is an ω-groundstate too for every $Z \subseteq I_\omega$. Hence, for almost every ω we have uncountably many ω-groundstates.

On the other hand, if the distribution of ω is the Gaussian, then the probability that $\omega(2n-1) = \omega(2n)$ is zero. Therefore, ω-groundstate is almost sure unique in this XOR-system. For this reason we require that for almost every ω the probability that $\omega(F) = 0$ is zero for every finite $F \subseteq M$. Therefore, we consider the following property of the distribution of ω which is stronger than the condition $\mathrm{P}\left(\omega(A) \neq 0 \text{ for all } A \in S_k\right) = 0$, but it is more handy and Gaussian distribution satisfies it.

Definition 1.28. Let M be a countable set. Let $\mathcal{Z}$ be the set of all $x \in \mathbb{R}^M$ for which there exists $k \in \mathbb{Z}^M \setminus \{(0,0,\dots)\}$ such that $k_m \neq 0$ for finitely many $m \in M$ and

$$\sum_{m \in M, k_m \neq 0} k_m x_m = 0.$$

The probability space $(\mathbb{R}^M, \mathbb{B}^M, \mathrm{P})$ is unique if $\mathrm{P}(\mathcal{Z}) = 0$.

Note that $\omega \in \mathcal{Z}$ if $A \subseteq M$ finite and $\omega(A) = 0$. Moreover, for every $A \subseteq M$ it holds that $\omega \in \mathcal{Z}$ if and only if $\omega_A \in \mathcal{Z}$.

Note that if distribution of ω is unique and symmetric, then $\mathrm{P}(\omega(A) \geq 0) = \frac{1}{2}$ for every nonempty and finite $A \subseteq M$, since $\mathrm{P}(\omega(A) \geq 0) = \mathrm{P}(\omega(A) \leq 0)$ by symmetry and $\mathrm{P}(\omega(A) = 0) = 0$ by uniqueness.

Let us prove that the uniqueness is well defined.

Proposition 1.29. *The set $\mathcal{Z}$ is measurable and* $\mathrm{P}(\mathcal{Z}) = 0$ *for the Gaussian distribution.*

Proof. The set $\mathcal{Z}$ is measurable because it is a countable union of linear spaces $\left\{x \in \mathbb{R}^M \mid kx = 0\right\}$ where $k \in Z^M \setminus \{(0,0,\dots)\}$ such that $k_m \neq 0$ for finitely many $m \in M$. Furthermore, every linear space $\left\{x \in \mathbb{R}^M \mid kx = 0\right\}$ has measure zero which implies that $\mathrm{P}(\mathcal{Z}) = 0$ for the Gaussian distribution. $\square$

Now, we prove that every finite XOR-system has a unique groundstate almost surely. This can be proven directly but first we prove one stronger property of a XOR-system. It says that the symmetric difference of two groundstates does not contain any set of S_k as a subset almost surely.

Proposition 1.30. *Let (M, S) be a XOR-system and a weight function ω be chosen from a unique distribution. There is almost surely no ω-groundstates $A, B \in S$ such that $A \triangle B$ contains a non-empty set of S_k as a subset.*

Proof. Let $A, B \in S$ be an ω-groundstates and $K \in S_k$ such that $K \subseteq A \triangle B$. Since $\omega_B(K) = (\omega_A)_{A \triangle B}(K) = -\omega_A(K)$, we have $\omega_A(K) = 0$. Hence, $\omega \in \mathcal{Z}$ and

$$\mathrm{P}\left(\exists \omega\text{-groundstates } A, B \in S, \exists C \in S_k : C \subseteq A \triangle B\right) \leq \mathrm{P}(\mathcal{Z}) = 0.$$

$\square$

Corollary 1.31. *Let (M, S) be a finite XOR-system and distribution of a weight function ω be unique. Then, ω-groundstate is almost surely unique.*

Proof. The symmetric difference of two groundstates belongs into S_k and last proposition implies the statement. □

The proof of Proposition 1.30 is very simple but it has many other consequences. For example, the complete infinite σ-XOR-system $(\mathbb{N}, 2^{\mathbb{N}})$ has unique groundstate almost surely, because the symmetric difference of every two difference states of $2^{\mathbb{N}}$ contains a finite subset of $\mathbb{N}$. Note that the complete σ-XOR-system has a physical interpretation: It is the cut system of one-dimensional lattice.

Newman and Stein [73] proved that multiple domain walls between groundstates in 2D lattice does not exist. Their Lemma 1 states that a domain wall in 2D lattice is infinite and contains no loops or dangling ends. This lemma also follows from Proposition 1.30.

Now, we prove that every state in an infinite σ-XOR-system is a groundstate with zero probability.

Proposition 1.32. *Let (M, S) be a σ-XOR-system and distribution of ω be unique, symmetric and random variables $(\omega(m))_{m\in M}$ be mutually independent. Then, M is infinite if and only if* $\mathrm{P}\left(A \text{ is } \omega\text{-groundstate}\right) = 0$ *for every $A \in S$.*

Proof. Let M be infinite. Then by Theorem 1.19, there exists a sequence $(M_n)_{n\in\mathbb{N}}$ of S_k, of pairwise different nonempty sets. Since random variables $(\omega(m))_{m\in M}$ are mutually independent, random variables $(\omega(M_n))_{n\in\mathbb{N}}$ are also mutually independent. Hence,

$$\begin{aligned}\mathrm{P}\left(A \text{ is } \omega\text{-groundstate}\right) &\le \mathrm{P}\left(\omega_A(M_n) \ge 0\ \forall n \in \mathbb{N}\right)\\ &= \prod_{n\in\mathbb{N}} \mathrm{P}\left(\omega_A(M_n) \ge 0\right) = \prod_{n\in\mathbb{N}} \frac{1}{2} = 0.\end{aligned}$$

Let M be finite. Then by Proposition 1.12, it holds that $S = S_k$ and S is finite. If $\mathrm{P}\left(A \text{ is } \omega\text{-groundstate}\right) = 0$ for all $A \in S$, then

$$1 = \mathrm{P}\left(\exists A \in S_\sigma : A \text{ is } \omega\text{-groundstate}\right) \le \sum_{A\in S_k} \mathrm{P}\left(A \text{ is } \omega\text{-groundstate}\right) = 0,$$

which is a contradiction. □

Let us present an example which shows that we cannot avoid the independence in the last statement. Let (M, S) be an infinite σ-XOR-system. Assume that $M = \mathbb{N}$ to simplify the notation. Let $\omega(1)$ be a random variable chosen from the Gaussian distribution and let $\omega(n) = e^{n-1}\omega(1)$ for all $n \in \mathbb{N}$ and for almost every $\omega \in \mathbb{R}^{\mathbb{N}}$. This distribution is symmetric; and moreover, it is unique because e is Euler constant which is transcendental. Therefore, weights of all elements of M have the same sign almost surely which implies that $\mathrm{P}\left(\emptyset \text{ is an } \omega\text{-groundstate}\right) = \frac{1}{2}$.

Now, we present other unnatural properties of $\pm J$ distribution. In $\pm J$ distribution the coupling constants are independently and uniformly chosen between two numbers $+1$ and -1. Crucial but physically unnatural property of this distribution is that it too often happen that a finite change of states (or, set of S_k) has weight zero. Hence, one can consider a sharp inequality in the definition of groundstate.

Definition 1.33. Let (M, S) be a XOR-system and let $\omega : M \to \mathbb{R}$ be a weight function. A state $A \in S$ is a sharp ω-groundstate if $\omega_A(B) > 0$ for every non-empty state $B \in S_k$.

In a unique distribution we do not need to distinguish between groundstates and sharp groundstates because every groundstate is almost surely sharp. But the situation is more complicated in $\pm J$ distribution.

Proposition 1.34. *Let graph $G = (V, E)$ be a cycle and let $(E, \mathcal{C}_G)$ be its cut system. If weight function $\omega : E \to \{\pm 1\}$ is chosen from $\pm J$ distribution, then there is no sharp ω-groundstate in $(E, \mathcal{C}_G)$ with probability $1/2$ and there are multiple ω-groundstates with probability $1/2$.*

Proof. Let $neg(\omega)$ be the set of edges $e \in E$ with $\omega(e) = -1$. Observe that cuts in the cycle are exactly sets of edges of even size. Note that $|neg(\omega_A)|$ has the same parity for every cut A. The probability that $|neg(\omega)|$ is odd is $1/2$.

Therefore, if $|neg(\omega)|$ is odd, then we find multiple ω-groundstates but no sharp one. Indeed, a cut A is an ω-groundstate if and only if A is even and $|A \triangle neg(\omega)| = 1$. On the other hand, if A would be a sharp ω-groundstate, then there exists an edge $e \in neg(\omega_A)$ and let f be any other edge but $\omega_A(\{e, f\}) = 0$.

If $|neg(\omega)|$ is even, then $A = neg(\omega)$ is the only ω-groundstate which is sharp because ω_A has no edge of negative weight. $\square$

In the last proposition we can notice that there is no sharp ω-groundstate if and only if there are multiple ω-groundstates for every $\omega : M \to \mathbb{R}$. This statement holds generally.

Proposition 1.35. *Let (M, S) be a XOR-system and $\omega : M \to \mathbb{R}$. There exists an ω-groundstate which is not sharp if and only if there exist ω-groundstates $A, B \in S$ such that $A \triangle B$ is finite and non-empty.*

Proof. Since A is not a sharp ω-groundstate, there exists $B \in S_k$ such that $\omega_A(B) = 0$. We prove that $A \triangle B$ is also an ω-groundstate. We use Lemma 1.22 to obtain

$$\omega_{A \triangle B}(C) = \omega_A(B \triangle C) - \omega_A(B) = \omega_A(B \triangle C) \geq 0,$$

since A is an ω-groundstate, where $C \in S_k$. Therefore, $\omega_{A \triangle B}(C) \geq 0$ for every $C \in S_k$ which proves that $A \triangle B$ is an ω-groundstate.

On the other hand, let $A, B \in S$ be ω-groundstates such that $A \triangle B$ is finite and non-empty. From definition it follows that $\omega(X) = -\omega_X(X)$ for every finite set $X \subseteq M$ which implies that

$$0 \leq \omega_A(A \triangle B) = -\omega_B(A \triangle B) \leq 0.$$

Hence, both A and B are ω-groundstates that are not sharp. $\square$

Proposition 1.36. *Let (M, S) be a finite XOR-system and $\omega : M \to \mathbb{R}$. There is no sharp ω-groundstate if and only if there exist at least two ω-groundstates.*

Proof. If there is no sharp ω-groundstate, then there are at least two ω-groundstates by Theorem 1.24 and Proposition 1.35.

For a contradiction, let us assume that there exist ω-groundstates $A, B \in S$ such that A is sharp. So,

$$0 \leq \omega_A(A \triangle B) = -\omega_B(A \triangle B) \leq 0.$$

Hence, A is not a sharp ω-groundstate. $\square$

Proposition 1.37. *Let graph $G = (V, E)$ be the 2-dimensional square lattice and let $(E, \mathcal{C}_G)$ be its cut system. If weight function $\omega : E \to \{\pm 1\}$ is chosen from $\pm J$ distribution, then there are at least two ω-groundstates in $(E, \mathcal{C}_G)$ almost surely but there is no sharp ω-groundstate almost surely.*

Proof. First, we prove that there is no ω-sharp groundstate almost surely. Then, the existence of at least two ω-groundstates follows from Proposition 1.35.

We split whole infinite lattice into infinitely many pair-wise disjoint finite sublattices. We present a particular configuration of weights ω on those finite sublattices which prevents the existence of a sharp ω-groundstate. Since we consider $\pm J$ distribution, such configuration occurs on each sublattice with positive probability. Hence, the probability that the configuration does not occur in any sublattice is zero.

So, it remains to present the configuration which prevents the existence of a sharp ω-groundstate. Let $neg(\omega, E')$ be the set of edges $e \in E'$ with $\omega(e) = -1$ where $E' \subseteq E$. Recall that $|neg(\omega_A, C)|$ and $|neg(\omega, C)|$ have the same parity for every cut A where C is a finite cycle in G. In the configuration of weights ω we prescribe parity of $|neg(\omega, C)|$ on some squares C. The configuration of parities in squares is described in Figure 1.1. Those prescribed parities remains in a sharp ω-groundstates.

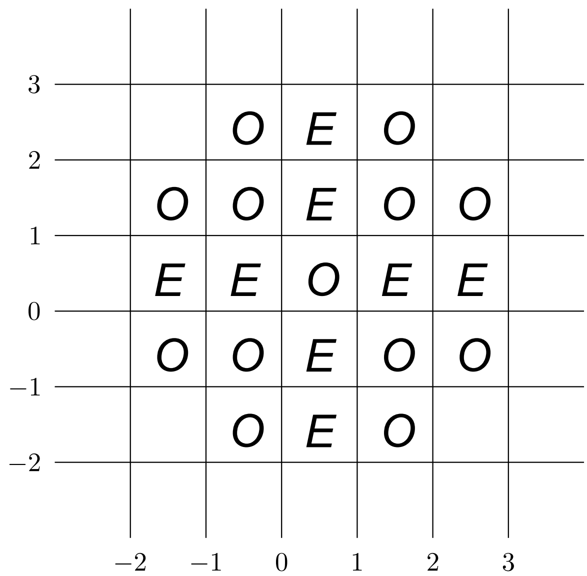


Figure 1.1: A configuration in a sublattice for Proposition 1.37. Letters "O" and "E" mean that the square has odd and even number of edges e with $\omega(e) = -1$, respectively.

In the rest of the proof, we use the following notation. Let $[a, b]$ be the vertex on coordinates a and b. Let $[a : a+1, b]$ be the edge between vertices $[a, b]$ and $[a+1, b]$, similarly $[a, b : b+1]$. Let $[a : a+1, b : b+1]$ be the square on edges $[a : a+1, b], [a+1, b : b+1], [a : a+1, b+1]$ and $[a, b : b+1]$.

Let A be a sharp ω-groundstate. We use two observations. First, every vertex is incident with at most one edge e with $\omega_A(e) = -1$ because every vertex has degree 4. Second, if $|neg(\omega_A, C)|$ is odd for a square C, then $|neg(\omega_A, C)| = 1$, because the only other possibility is $|neg(\omega_A, C)| = 3$ which volatiles the first observation for some vertex on the square C.

By the second observation we know that $|neg(\omega_A, [0 : 1, 0 : 1])| = 1$. Since the configuration is symmetric, we assume without lost of generality that $\omega_A([1, 0 : 1]) = -1$

and other edges on the square $[0:1,0:1]$ have positive weight. From the first observation it follows that all edges incident with vertices $[1,0]$ and $[1,1]$ except the edge $[1,0:1]$ have positive weight because $\omega_A([1,0:1]) = -1$. Next, $\omega_A([2,0:1]) = -1$ because $|neg(\omega_A,[1:2,0:1])|$ is even and all other edges have known weight. From the first observation it follows that all edges incident with vertices $[2,0]$ and $[2,1]$ except the edge $[2,0:1]$ have positive weight because $\omega_A([2,0:1]) = -1$. Again, $\omega_A([3,0:1]) = -1$ because $|neg(\omega_A,[2:3,0:1])|$ is even and all other edges have known weight. For the last time, from the first observation it follows that all edges incident with vertices $[3,0]$ and $[3,1]$ except the edge $[3,0:1]$ have positive weight because $\omega_A([3,0:1]) = -1$. Finally, all edges on squares $[1:2,1:2]$ and $[2:3,1:2]$ except $[1:2,2]$ and $[2:3,2]$ have positive weight, which implies that $\omega_A([1:2,2]) = \omega_A([2:3,2]) = -1$ which contradicts the first observation on vertex $[2,2]$. This concludes the proof. □

1.7 Transitive XOR-systems

A graph $G = (V,E)$ is vertex transitive if for every $u,v \in V$ there exists a graph automorphism $f : V \to V$ on G such that $f(u) = v$. Similarly, G is edge transitive if for every $d,e \in E$ there exists a graph automorphism $f : V \to V$ on G such that $f(d) = e$. A lattice is a vertex and edge transitive graph. In this section we describe this property on XOR-systems.

Definition 1.38. We say that XOR-systems (M_1,S_1) and (M_2,S_2) are isomorphic if there exists a bijection $f : M_1 \to M_2$ such that $A \in S_1$ if and only if $f(A) \in S_2$ for every $A \subseteq M_1$. Such function f is called an isomorphism between (M_1,S_1) and (M_2,S_2). An isomorphism between (M_1,S_1) and (M_1,S_1) is called an automorphism on (M_1,S_1). A XOR-system (M_1,S_1) is transitive if for every $m,n \in M_1$ there exists an automorphism $f_{m,n}$ on (M_1,S_1) such that $f_{m,n}(m) = n$.

Clearly, cut systems of common lattices (i.e. n-dimensional square lattice, hexagonal lattice) form transitive σ-XOR-systems. Let

$$\mathcal{G} := \{\omega : M \to \mathbb{R} \mid \exists A,B \ \omega\text{-groundstates: } A \neq B\}$$

and

$$\mathcal{G}_m := \{\omega : M \to \mathbb{R} \mid \exists A,B \ \omega\text{-groundstates: } m \in A \triangle B\}$$

where $m \in M$. So, $\mathrm{P}(\mathcal{G})$ is the probability that there exist two different groundstates and $\mathrm{P}(\mathcal{G}_m)$ is the probability that there exist two groundstates whose symmetric difference contains given element. Note that $\mathrm{P}(\mathcal{G}) = \mathrm{P}(\cup_{m\in M}\mathcal{G}_m)$.

Lemma 1.39. *Let (M,S) be a transitive XOR-system and the distribution of weight function ω be independently and identically distributed. Then, $\mathrm{P}(\mathcal{G}_n) = \mathrm{P}(\mathcal{G}_m)$ for every $m,n \in M$.*

Proof. Let $f_{m,n}$ be an automorphism on (M,S) such that $f_{m,n}(m) = n$. Observe, that $\mathcal{G}_n$ is the set of all weight functions $\omega' : M \to \mathbb{R}$ such that $\omega'(x) = \omega(f_{m,n}(x))$ for all $x \in M$ where $\omega \in \mathcal{G}_m$. Therefore, $\mathrm{P}(\mathcal{G}_n) = \mathrm{P}(\mathcal{G}_m)$. □

Let (M, S) be a transitive σ-XOR-system. Let the weight function $\omega : M \to \mathbb{R}$ be chosen from an independent and identical distribution. Let $\alpha = \mathrm{P}(\mathcal{G}_n)$ for any $n \in M$. We prove that if $\alpha = 0$ then the probability that there exist two different groundstates is zero. It implies that there are no incongruent groundstates if $\alpha = 0$.

Theorem 1.40. *Let (M, S) be a transitive XOR-system and let the distribution of weight function ω be independent and identical. Then, $\alpha = 0$ if and only if $\mathrm{P}(\mathcal{G}) = 0$.*

Proof. If $\mathrm{P}(\mathcal{G}) = 0$, then $\alpha = 0$ because $\mathcal{G}_m \subseteq \mathcal{G}$ for every $m \in M$.

Let us assume that $\alpha = 0$. Since M is countable we can use the sub-additivity to obtain

$$\begin{aligned} \mathrm{P}(\exists A, B \ \omega\text{-grounstates: } A \neq B) &= \mathrm{P}(\exists A, B \ \omega\text{-grounstates } \exists m \in M : m \in A \triangle B) \\ &= \mathrm{P}\left(\bigcup_{m \in M} \mathcal{G}_m\right) \leq \sum_{m \in M} \mathrm{P}(\mathcal{G}_m) = \sum_{m \in M} \alpha = 0. \end{aligned}$$

□

Note that there exist two different groundstates with probability at least α. Now, we prove that $\alpha < 1$.

Lemma 1.41. *Let (M, S) be a XOR-system, $K \in S_k$, $m \in K$ and $\omega : M \to \mathbb{R}$. If*

$$|\omega(m)| > \sum_{x \in K \setminus \{m\}} |\omega(x)|, \tag{1.2}$$

then there do not exist ω-groundstates $A, B \in S$ such that $m \in A \triangle B$.

Proof. First, observe that (1.2) is equivalent to (1.3).

$$\forall C \subseteq M : \ |\omega(m)| > \omega_C(K \setminus \{m\}) \tag{1.3}$$

For a contradiction, let us assume that there exist ω-groundstates $A, B \in S$ such that $m \in A \triangle B$. Without lost of generality, assume that $m \in A \setminus B$.

If $\omega(m) > 0$, then $0 \leq \omega_A(K) = \omega_A(m) + \omega_A(K \setminus \{m\}) = -\omega(m) + \omega_A(K \setminus \{m\})$ since A is an ω-groundstate which contradicts (1.3).

If $\omega(m) < 0$, then $0 \leq \omega_B(K) = \omega_B(m) + \omega_B(K \setminus \{m\}) = \omega(m) + \omega_B(K \setminus \{m\})$ since B is an ω-groundstate which also contradicts (1.3). □

Theorem 1.42. *Let (M, S) be a transitive σ-XOR-system and let distribution of $\omega : M \to \mathbb{R}$ be the independent and identical Gaussian distribution. Then, $\alpha < 1$.*

Proof. Let $m \in M$. By Proposition 1.18, there exists $K \in S_k$ containing m. Since we consider the Gaussian distribution, we know that $\mathrm{P}((1.2) \text{ holds}) > 0$. Therefore, $\alpha = \mathrm{P}(\mathcal{G}_m) \leq 1 - \mathrm{P}((1.2) \text{ holds}) < 1$. □

1.8 Domain walls

Proposition 1.32 states that every state is a groundstate with probability zero in infinite σ-XOR-systems. In this section we study the probability that a state is a domain wall, that is, a state is a symmetric difference of two groundstates. By Corollary 1.31, every finite XOR-system has a unique groundstate almost surely, so we restrict our attention in infinite σ-XOR-systems.

Let (M, S) be a XOR-system. We say that a sequence $(A_n)_{n\in\mathbb{N}}$ of S_k has bounded size if $\max_{n\in\mathbb{N}} |A_n|$ is finite.

We prove that a state is not a symmetric difference of two groundstates almost surely only for transitive σ-XOR-systems and cut systems (M, S) because our proof uses a sequence $(A_m)_{m\in M}$ of S_k with bounded size such that $m \in A_m$ for every $m \in M$. Such sequence does not exist in general σ-XOR-system, for example, the σ-XOR-system on $\mathbb{N}$ generated by sets

$$\{1\}, \{2, 3\}, \{4, 5, 6\}, \{7, 8, 9, 10\}, \ldots.$$

Lemma 1.43. *Let (M, S) be a transitive σ-XOR-system. There exists a sequence $(A_m)_{m\in M}$ of S_k with bounded size such that $m \in A_m$ for every $m \in M$.*

Proof. Let us choose $m' \in M$. By Proposition 1.18, there exists $A' \in S_k$ containing m'. Since (M, S) is transitive, there exists an automorphism f_m on (M, S) such that $f_m(m') = m$ for all $m \in M$. Let A_m be $f_m(A')$. Note that $m \in A_m$ for all $m \in M$ and all sets $(A_m)_{m\in M}$ have the same size. □

Lemma 1.44. *Let $(E, \mathcal{C}_G)$ be a cut system of a graph $G = (V, E)$ with bounded degree. There exists a sequence $(A_m)_{m\in E}$ of $\mathcal{C}_G$ with bounded size such that $m \in A_m$ for every $m \in E$.*

Proof. For every edge $m = uv$ let A_m be the set of edges incident with the vertex u. Since the graph G has bounded degree, the sequence $(A_m)_{m\in E}$ has sets of bounded size. □

Lemma 1.45. *Let (M, S) be an infinite σ-XOR-system which has a sequence $(A_m)_{m\in M}$ of S_k with bounded size such that $m \in A_m$ for all $m \in M$. Then, for every infinite set $C \subseteq M$ there exists a sequence $(C_n)_{n\in\mathbb{N}}$ of S_k of pair-wise disjoint sets with bounded size such that $C_n \cap C \neq \emptyset$ for every $n \in \mathbb{N}$.*

Proof. First, we construct an infinite subsequence $(B_n)_{n\in\mathbb{N}}$ of the sequence $(A_m)_{m\in M}$ which moreover has pair-wise different sets. Note that the sequence $(A_m)_{m\in C}$ has infinitely many different sets because $C \subseteq \bigcup_{m\in C} A_m$ is infinite. We consider a subsequence $(B_n)_{n\in\mathbb{N}}$ of the sequence $(A_m)_{m\in C}$ which has exactly one occurrence of each set of $(A_m)_{m\in C}$. Since $m \in A_m$ for all $m \in M$, let $(b_n)_{n\in\mathbb{N}}$ be the sequence of corresponding elements of M which satisfies $b_n \in B_n$ for every $n \in \mathbb{N}$. Hence, the sequence $(B_n)_{n\in\mathbb{N}}$ has similar properties as $(A_n)_{n\in\mathbb{N}}$. It is a sequence of pair-wise different sets of S_k with bounded size and for all $n \in \mathbb{N}$ it holds that $b_n \in B_n \cap C$.

We construct the desired sequence $(C_n)_{n\in\mathbb{N}}$ by induction. Let C_1 be B_1. Let us assume that $C_1, \ldots, C_k \in S_k$ are pair-wise disjoint sets such that $C_n \cap C \neq \emptyset$ for every $n \in \{1, \ldots, k\}$. Let D_k be $\bigcup_{n=1}^{k} C_n$. We find $C_{k+1} \in S_k$ such that $C_{k+1} \cap D_k = \emptyset$ and $C_{k+1} \cap C \neq \emptyset$.

Let E_k be the set of indexes $n \in \mathbb{N}$ such that $b_n \notin D_k$. Let us consider the sequence $(B_n \cap D_k)_{n \in E_k}$. Since D_k is finite and E_k is infinite, $(B_n \cap D_k)_{n \in E_k}$ is an infinite sequence of finitely many sets. Therefore, there exists an infinite set $F_k \subseteq E_k$ such that $(B_n \cap D_k)_{n \in F_k}$ is a constant sequence. Hence, $(B_i \bigtriangleup B_j) \cap D_k = \emptyset$ for every $i, j \in F_k$.

It remains to find $i, j \in F_k$ such that $(B_i \bigtriangleup B_j) \cap C \neq \emptyset$. But it is easy to prove a stronger claim: For every $i \in F_k$ there exists $j \in F_k$ such that $b_j \notin B_i$. It holds because B_i is finite and F_k is infinite. Since $b_j \in B_j \cap C$ we know that $b_j \in (B_i \bigtriangleup B_j) \cap C$.

Note that $\max_{n \in \mathbb{N}} |C_n| \leq 2 \max_{m \in M} |A_m|$ because every set of $(C_n)_{n \in \mathbb{N}}$ is defined as a symmetric difference of (at most) two sets of $(A_m)_{m \in M}$. This finishes the proof. $\square$

Proposition 1.46. *Let (M, S) be an infinite σ-XOR-system and let A be an infinite set of S. Let $(A_n)_{n \in \mathbb{N}}$ be a sequence of S_k of pair-wise disjoint sets with bounded size such that $A_n \cap A \neq \emptyset$ for every $n \in \mathbb{N}$. Let a weight function $\omega : M \to \mathbb{R}$ be chosen from the independent and identical Gaussian distribution. Then,*

$$\mathrm{P}\left(\exists B \in S : B, A \bigtriangleup B \text{ are } \omega\text{-groundstates}\right) = 0.$$

Proof. First, observe that

$$\begin{aligned}
&\mathrm{P}\left(\exists B \in S : B, A \bigtriangleup B \text{ are } \omega\text{-groundstates}\right) \\
&\qquad \leq \mathrm{P}\left(\exists B \in S : \omega_B(A_n) \geq 0,\ \omega_{A \bigtriangleup B}(A_n) \geq 0 \ \ \forall n \in \mathbb{N}\right) \\
&\qquad\qquad \leq \mathrm{P}\left(\exists B \subseteq M : \omega_B(A_n) \geq 0,\ \omega_{A \bigtriangleup B}(A_n) \geq 0 \ \ \forall n \in \mathbb{N}\right).
\end{aligned}$$

The formula "$\exists B \subseteq M$" says that we have to change signs of ω to satisfy conditions $\omega_B(A_n) \geq 0$ and $\omega_{A \bigtriangleup B}(A_n) \geq 0$. Since sets $(A_n)_{n \in \mathbb{N}}$ are pair-wise disjoint, we can choose signs of ω independently for every A_n. Hence,

$$\begin{aligned}
&\mathrm{P}\left(\exists B \subseteq M : \omega_B(A_n) \geq 0,\ \omega_{A \bigtriangleup B}(A_n) \geq 0 \ \ \forall n \in \mathbb{N}\right) \\
&\qquad = \prod_{n \in \mathbb{N}} \mathrm{P}\left(\exists B \subseteq M : \omega_B(A_n) \geq 0,\ \omega_{A \bigtriangleup B}(A_n) \geq 0\right).
\end{aligned}$$

Let

$$P_n = \mathrm{P}\left(\exists B \subseteq M : \omega_B(A_n) \geq 0,\ \omega_{A \bigtriangleup B}(A_n) \geq 0\right).$$

If we prove that $P_n \leq c$ for some constant $c < 1$ which does not depend on n, then $\mathrm{P}\left(\exists B \in S : B, A \bigtriangleup B \text{ are } \omega\text{-groundstates}\right) = 0$.

In the probability P_n we have two conditions

$$\omega_B(A_n) = \omega_B(A_n \setminus A) + \omega_B(A_n \cap A) \geq 0$$

and

$$\omega_{B \bigtriangleup A}(A_n) = \omega_B(A_n \setminus A) - \omega_B(A_n \cap A) \geq 0$$

which we simplify into one condition

$$\omega_B(A_n \setminus A) \geq |\omega_B(A_n \cap A)|.$$

Let $t_n = |A_n \cap A|$ and $r_n = |A_n \setminus A|$. Let $X_1, \ldots, X_{t_n}$ and $Y_1, \ldots, Y_{r_n}$ be random variables $(\omega(m))_{m \in A_n \cap A}$ and $(\omega(m))_{m \in A_n \setminus A}$, respectively. Since $A_n \cap A$ is non-empty, $t_n \geq 1$. If $r_n = 0$, then $P_n = 0$ by Proposition 1.30. We assume that $r_n \geq 1$.

In order to prove that the probability that $|\omega_B(A_n \cap A)| \geq 1$ for all $B \subseteq M$ is positive, we consider the event that $|X_i|$ is close to 2^i for every $i \in \{1, \dots, t_n\}$. Observe that if $|X_i|$ and 2^i differ less than $\frac{1}{t_n}$ for all $i \in \{1, \dots, t_n\}$, then $|\omega_B(A_n \cap A)| > 1$. Because the distribution of ω is Gaussian, we know that

$$\mathrm{P}\left(\forall B \subseteq M : |\omega_B(A_n \cap A)| > 1\right) \geq \mathrm{P}\left(\left|X_i - 2^i\right| < \frac{1}{t_n} \quad \forall i = 1, \dots, t_n\right) > 0.$$

On the other hand, if $|Y_i| \leq \frac{1}{r}$ for every $i \in \{1, \dots, r_n\}$, then $|\omega_B(A_n \setminus A)| < 1$ for every $B \subseteq M$. Hence,

$$\mathrm{P}\left(\forall B \subseteq M : |\omega_B(A_n \setminus A)| < 1\right) \geq \mathrm{P}\left(|Y_i| < \frac{1}{r_n} \quad \forall i = 1, \dots, r_n\right) > 0.$$

All together, we have

$$\begin{aligned}
P_n &= \mathrm{P}\left(\exists B \subseteq M : \omega_B(A_n \setminus A) \geq |\omega_B(A_n \cap A)|\right) \\
&= 1 - \mathrm{P}\left(\forall B \subseteq M : \omega_B(A_n \setminus A) < |\omega_B(A_n \cap A)|\right) \\
&\leq 1 - \mathrm{P}\left(\forall B \subseteq M : \omega_B(A_n \setminus A) < 1 < |\omega_B(A_n \cap A)|\right) \\
&= 1 - \mathrm{P}\left(\forall B \subseteq M : |\omega_B(A_n \setminus A)| < 1)\right) \cdot \mathrm{P}\left(\forall B \subseteq M : |\omega_B(A_n \cap A)| > 1\right) \\
&\leq 1 - \mathrm{P}\left(|Y_i| < \frac{1}{r_n} \quad \forall i = 1, \dots, r_n\right) \cdot \mathrm{P}\left(\left|X_i - 2^i\right| < \frac{1}{t_n} \quad \forall i = 1, \dots, t_n\right) \\
&< 1.
\end{aligned}$$

Hence, $P_n < 1$ and moreover, the probability P_n depends only on r_n and t_n. Since the sequence $(A_n)_{n \in \mathbb{N}}$ has sets of bounded size, there are finitely many different combination of values r_n and t_n, and we define c to be the maximal value of P_n. Hence, we have $c < 1$ such that $P_n \leq c$ for every $n \in \mathbb{N}$ which concludes the proof. □

Theorem 1.47. *Let (M, S) be an infinite transitive σ-XOR-system or a cut system of a graph with bounded degree. Let distribution of $\omega : M \to \mathbb{R}$ be the independent and identical Gaussian distribution. Let $A \in S$. Then,*

$$\mathrm{P}\left(\exists B \in S : B, A \triangle B \text{ are } \omega\text{-groundstates}\right) = \begin{cases} 0 & \text{if } A \text{ is non-empty,} \\ 1 & \text{otherwise.} \end{cases}$$

Proof. If A is the empty set, then the statement only says that there (almost surely) exists a groundstate which follows from Theorem 1.24. If A non-empty and finite, then the statement follows from Proposition 1.30. Let us assume that A is infinite.

By Lemmas 1.43 and 1.44 there exists a sequence $(A_m)_{m \in M}$ of S_k with bounded size such that $m \in A_m$ for every $m \in M$. By Lemma 1.45 there exists a sequence $(A_n)_{n \in \mathbb{N}}$ of S_k of pair-wise disjoint sets with bounded size such that $A_n \cap A \neq \emptyset$ for every $n \in \mathbb{N}$. Finally, from Proposition 1.46 we conclude that

$$\mathrm{P}\left(\exists B \in S : B, A \triangle B \text{ are } \omega\text{-groundstates}\right) = 0.$$

□

1.9 Conclusions

We study groundstates in a generalization of Edwards-Anderson Ising model. The original motivation of Ising model is ferromagnetism in critical structures which form lattices or grids but the concept of Hamiltonian

$$H(\sigma) = -\sum_{\langle i,j\rangle} J_{ij}\sigma_i\sigma_j$$

and groundstates makes mathematical sense in an arbitrary graph.

A groundstate is a state σ of locally minimal Hamiltonian. The Hamiltonian is essentially a sum over all edges of their weights multiplied by 1 or -1. But we cannot choose arbitrary set of edges whose weight we want to multiply by -1 in the Hamiltonian. We can choose only those sets of edges which form cuts in the graph. A groundstate is also a cut which leads us to study cut systems $(E, \mathcal{C}_G)$ where $G = (V, E)$ is a graph on countably many vertices with bounded degree and $\mathcal{C}_G$ is the family of all cuts of G.

For our convenience, we denote the coupling constants J by a weight function $\omega : E \to \mathbb{R}$. A sum $\sum_{e\in A} \omega(e)$ is denoted by $\omega(A)$, and ω_A is the weight function obtained from ω by flipping the sings on all edges of A, where $A \subseteq E$ (Definition 1.2). In this terminology and notation, a cut A is an ω-groundstate if $\omega_A(B) \geq 0$ for every finite cut B (Definition 1.1).

The essential property of a cut system is the closure on symmetric differences; i.e. the symmetric difference of every pair of cuts is a cut also. We focus our attention on this property and say that (M, S) is a XOR-system if M is a countable ground set and S is a family of subsets of M which is closed under finite symmetric differences (Definition 1.5). It is clear that every cut system forms a XOR-system.

It is quite unnatural to consider only finite symmetric differences. Therefore, we define a limit and a symmetric difference of a sequence of S by the classical way in Definitions 1.6 and 1.7. We restrict our attention on limits instead of symmetric differences of sequences because it is more convenient and Proposition 1.9 proves that a XOR-system contains limits of all converging sequences of S if and only if it contains symmetric differences of sequences of S.

We consider XOR-systems (M, S) that contain limits of converging sequences of S (Definition 1.8). This gives us a very useful tool called compactness (Theorem 1.17). Let S_k be the set of all finite sets of S. Let S_σ be the sets of all limits of converging sequences of S_k. We say that a XOR-system is a σ-XOR-system if it is closed under limits and $S = S_\sigma$ (Definition 1.10). Theorem 1.15 shows that every cut system is a σ-XOR-system which is one of the reasons why we are mainly interested in σ-XOR-systems.

Another interesting property of S_σ is that S_σ does not contain only all limits of converging sequences of S_k but also limits of converging sequences of S_σ by Lemma 1.13. Moreover, Proposition 1.14 states that for a XOR-system (M, S) which is closed under limits it holds that (M, S_σ) is a σ-XOR-system.

We can use S_σ for factorization of a σ-XOR-system (M, S). Let $A, B \in S$ be in a relation σ if $A \triangle B \in S_\sigma$. The relation σ is an equivalence which factorizes S into classes S/σ. The translation invariance of a σ-XOR-system (M, S) also shows that classes S_1 and S_2 of S/σ are the same because there is the bijection between $B \in S_1$ and $B \triangle A_1 \triangle A_2 \in S_2$ where $A_1 \in S_1$ and $A_2 \in S_2$. These classes are crucial for groundstates.

We say that $A \in S$ is an ω-groundstate in a XOR-system (M, S) where $\omega : M \to \mathbb{R}$ if $\omega_A(B) \geq 0$ for all $B \in S_k$ (Definition 1.20). Note that this definition only extends the definition of groundstates in cut systems into more general set systems. Theorem 1.24 proves that an ω-groundstate exists in every σ-XOR-system (M, S) and every $\omega : M \to \mathbb{R}$. Moreover, Corollary 1.25 shows that the translation invariance gives us an ω-groundstate in every class S/σ of a XOR-system (M, S) which is closed under limits. This leads us to study groundstates in σ-XOR-systems and ask whether groundstates are unique in σ-XOR-systems.

A XOR-system (M, S) is finite if M is finite; otherwise, (M, S) is infinite. We present dichotomy between finite and infinite σ-XOR-systems. Proposition 1.12 proves that a finite XOR-system (M, S) is a σ-XOR-system and $S = S_k = S_\sigma$ and they are finite. On the other hand, if (M, S) is an infinite σ-XOR-system, then S_k is infinite and S_σ is uncountable by Theorem 1.19.

We know that an ω-groundstate always exists in a σ-XOR-system (M, S) and we are interested whether the ω-groundstate is unique almost surely. This question depends on the distribution function of $\omega : M \to \mathbb{R}$. The most common distributions are independent and identical Gaussian and $\pm J$ distributions. Generally, the distribution of ω is symmetric around zero (Definition 1.27).

The unnatural property of $\pm J$ distribution is that $\mathrm{P}(\omega(B) = 0)$ is positive for every $B \in S_k$. Moreover, Proposition 1.37 shows that an ω-groundstate is not unique in 2D lattice if ω is chosen from $\pm J$ distribution. On the other hand, there is almost surely no cut A such that $\omega_A(B) > 0$ for every finite and non-empty cut B. But for Gaussian distribution, every ω-groundstate $A \in S$ almost surely satisfies the stronger condition $\omega_A(B) > 0$ for every non-empty $B \in S$ in every σ-XOR-system (M, S). This leads us to Definition 1.28 of unique distribution which ensures that $\omega(B) \neq 0$ for all $B \in S_K$ almost surely.

Proposition 1.30 claims that if a weight function ω is chosen from a unique distribution, there are almost surely no pair of ω-groundstates $A, B \in S$ such that $A \triangle B$ contains a non-empty set of S_k as a subset.

We say that a XOR-system (M, S) is transitive if for every $m, n \in M$ there exists a bijection $f : M \to M$ such that $f(m) = n$ and for every $A \subseteq M$ it holds that $A \in S$ if and only if $f(A) \in S$ (Definition 1.38). A typical example of a transitive σ-XOR-system is the cut system of a lattice. Let $\mathrm{P}(\mathcal{G}_m)$ be the probability that there exist two ω-groundstates whose symmetric difference contains $m \in M$. It is not surprising that $\mathrm{P}(\mathcal{G}_m) = \mathrm{P}(\mathcal{G}_n)$ for every $m, n \in M$ in a transitive XOR-system and ω chosen from an independent and identical distribution (Lemma 1.39). It may be more interesting that $\mathrm{P}(\mathcal{G}_m) = 0$ if and only if ω-groundstate is almost surely unique under the assumptions that ω chosen from an independent and identical distribution (Theorem 1.40). Furthermore, $\mathrm{P}(\mathcal{G}_m) < 1$ if the weight function is chosen from the independent and identical Gaussian distribution (Theorem 1.42).

We study the probabilities that a given state is a groundstate and also a symmetric difference of two groundstates. Both probabilities are zero in infinite σ-XOR-systems under the following assumptions. By Proposition 1.32, a state of S is not almost surely an ω-groundstate if the distribution of ω is unique, symmetric and independent. By Theorem 1.47, for every state of $A \in S$ the probability that there exist two ω-groundstates $B, C \in S$ such that $A = B \triangle C$ is zero, if (M, S) is an infinite transitive σ-XOR-system or a cut system of a graph with bounded degrees and the distribution of ω is the independent and identical Gaussian distribution.

Our study of XOR-systems convince us to believe in uniqueness of groundstate.

Conjecture 1.48. *Let (M, S) be a transitive σ-XOR-system and weight function ω be chosen from the independent and identical Gaussian distribution. Then, ω-groundstate is almost surely unique.*

Furthermore, we do not know any example of a σ-XOR-system having multiple ω-groundstates with positive probability if the distribution of ω is independent, unique and symmetric.

Part III

Perfect matchings

Chapter 2

Introduction

A set of edges $P \subset E$ of a graph $G = (V, E)$ is a *matching* if every vertex of G is incident with at most one edge of P. If a vertex v of G is incident with an edge of P, we say that v is *covered* by P. A matching P is *perfect* if every vertex of G is covered by P.

The d-dimensional hypercube Q_d is a graph whose vertex set consists of all binary vectors of length d, with two vertices being adjacent whenever the corresponding vectors differ at exactly one coordinate. The binary vectors are labelled by the set $[d] := \{1, 2, \ldots, d\}$.

It is well known that Q_d is Hamiltonian for every $d \geq 2$. This statement can be traced back to 1872 [50]. Since then the research on Hamiltonian cycles in hypercubes satisfying certain additional properties has received considerable attention. An interested reader can find more details about this topic in the survey of Savage [80], e.g. Dvořák [23] showed that any set of at most $2d - 3$ edges of Q_d ($d \geq 2$) that induces vertex-disjoint paths is contained in a Hamiltonian cycle. Dimitrov et al. [21] proved that for every perfect matching P of Q_d ($d \geq 3$) there exists a Hamiltonian cycle that faults P, if and only if P is not a layer of Q_d.

Every Hamiltonian cycle of Q_d can be split into 2 perfect matchings. Therefore, it is natural to ask the opposite question whether every perfect matching of Q_d can be extended into a Hamiltonian cycle. As far as we know, the first mention of this question was published by Kreweras [59] who conjectured that answer to this question is positive. Independently, this problem was stated by Donald E. Knuth [57, problem 7.2.1.1–55].

Conjecture 2.1 (Kreweras [59]). *Every perfect matching in the d-dimensional hypercube with $d \geq 2$ extends to a Hamiltonian cycle.*

We proved Conjecture 2.1 in paper [35]. We present the original proof [35] in Chapter 3. An interested reader may notice that the proof gives at least $2^{2^{d-4}}$ Hamiltonian cycles that extend given perfect matching of Q_d. This is one example of usefulness of our proof. Other applications of the proof are presented in next chapters.

Let $K(Q_d)$ be the complete graph on the vertices of the hypercube Q_d. If G is bipartite and connected, then let $B(G)$ be the complete bipartite graph with the same color classes as G. The main trick of our proof is that we proved a stronger statement: Every perfect matching of $K(Q_d)$ can be extended into a Hamiltonian cycle of $K(Q_d)$ using only edges of Q_d. This allows us to use an induction by dimension in a very simple way.

Ruskey and Savage [79, page 19, question 3] asked the following more general question which is still open.

Question 2.2. *Does every (not necessarily perfect) matching of Q_d for $d \geq 2$ extend to a Hamiltonian cycle of Q_d?*

The statement can be shown to be true for $d = 2, 3, 4$. However, our approach does not seem to lead to proving this stronger statement.

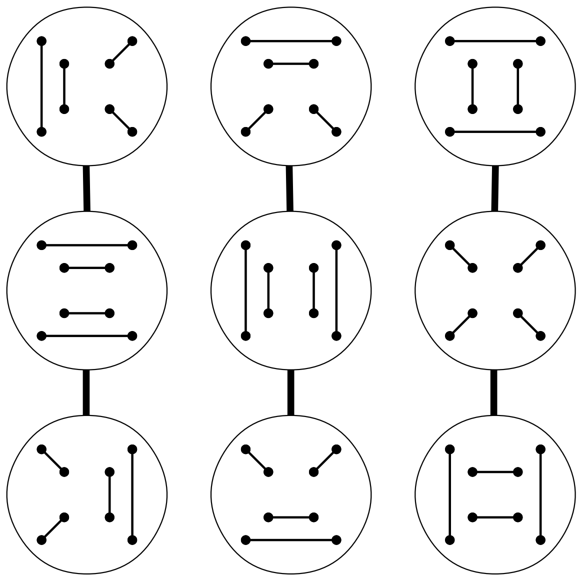


Figure 2.1: The matching graph $\mathcal{M}(Q_3)$. The circles and bold lines are vertices and edges of $\mathcal{M}(Q_3)$.

The *matching graph* $\mathcal{M}(G)$ of a graph G on an even number of vertices has a vertex set of all perfect matchings of G, with two vertices being adjacent whenever the union of the corresponding perfect matchings forms a Hamiltonian cycle of G; e.g. Figure 2.1 shows the matching graph $\mathcal{M}(Q_3)$. There is a natural one-to-one correspondence between Hamiltonian cycles of G and edges of $\mathcal{M}(G)$. The problems of determining the number $h(d)$ of Hamiltonian cycles of Q_d and the number of perfect matchings of Q_d, are well-known open problems. Douglas [22] presented upper and lower bounds

$$\left(\prod_{i=5}^{d-1} i^{2^{d-i-1}}\right) d(1344)^{2^{d-4}} 2^{2^{d-2}-1-d} \leq h(d) \leq \left(\frac{d(d-1)}{2}\right)^{2^{d-1}-2^{d-1-\log_2(d)}}.$$

Feder and Subi [34] presented the following bounds

$$\left(\left(\frac{d\log 2}{e\log\log d}\right)(1-o(1))\right)^{(2^d)} \leq h(d) \leq \frac{1}{2}(d!)^{\frac{2^d}{2d}}((d-1)!)^{\frac{2^d}{2(d-1)}}.$$

Independently, Fisher [43] and Kasteleyn [55] proved that the number of perfect matchings of G is the permanent of $A(G)$ when G is a balanced bipartite graph with adjacency matrix $A(G)$. Brègman [10] proved the conjecture of Minc [71] that for any $n \times n$ $0,1$-matrix A with row sums $r_1, \ldots, r_n$, the permanent of A is at most

$\prod_{i=1}^{n}(r_i!)^{1/r_i}$. In particular, a d-regular bipartite graph on n vertices has at most $(d!)^{n/(2d)} = \left(\frac{d}{e}(1+o(1))\right)^{n/2}$ perfect matchings.

Independently, Egoryĉev [28] and Falikman [30] proved the conjecture of van der Waerden [85] that for any doubly stochastic $n \times n$ matrix A the permanent of A is at least $\frac{n!}{n^n}$. This was used by Clark, George and Porter [17] to show that the number of perfect matchings of a d-regular bipartite graph on n vertices is at least $\left(\frac{2d}{n}\right)^{n/2}\left(\frac{n}{2}\right)! = \left(\frac{d}{e}(1+o(1))\right)^{n/2}$ perfect matchings.

Knowledge of structural properties of $\mathcal{M}(Q_d)$ may help to improve those bounds and give us other informations about Hamiltonian cycles of hypercubes.

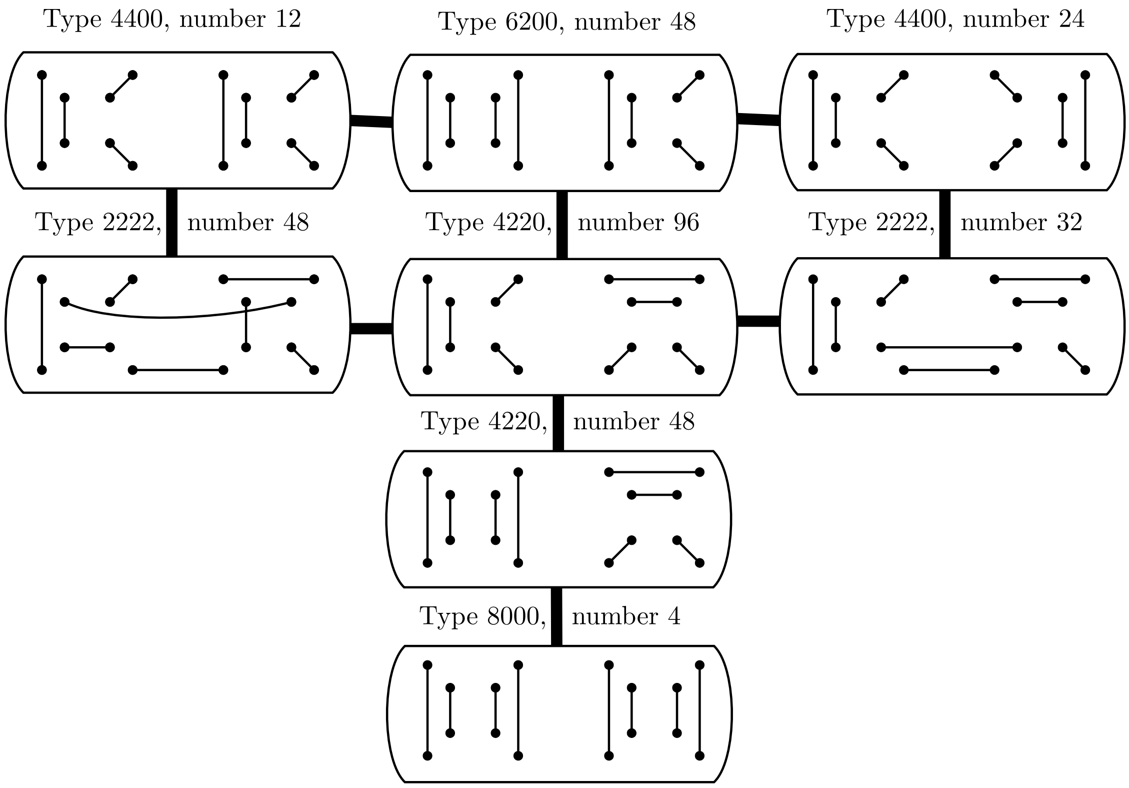


Figure 2.2: The graph M_4. For every equivalence class $[P]$ of isomorphism there is a frame which contains P. Four type digits above each frame are numbers of edges crossing each dimension. Above each frame there is also a number of perfect matchings which are contracted to the equivalence class.

We say that two perfect matchings P and R of Q_d are isomorphic if there exists an isomorphism $f : V(Q_d) \to V(Q_d)$ such that $f(u)f(v) \in R$ for every edge $uv \in P$. This relation of isomorphism is an equivalence and it partitions the set of all perfect matchings. Kreweras [59] considered a graph M_d which is obtained from $\mathcal{M}(Q_d)$ by contracting all vertices of each class of this equivalence. For example, Q_3 has two non-isomorphic perfect matchings, so M_3 has two vertices connected by an edge. The graph M_4 is presented on Figure 2.2. Kreweras [59] proved by inspection of all perfect matchings that the graphs M_3 and M_4 are connected and he conjectured that M_d is connected for $d \geq 3$.

Conjecture 2.3 (Kreweras [59]). *Graphs M_d are connected for every $d \geq 3$.*

It is more general to also ask whether the graph $\mathcal{M}(Q_d)$ is connected since the connectivity of $\mathcal{M}(Q_d)$ implies the connectivity of M_d. The answer is negative for

$d = 3$ (see Figure 2.1). However, we [36] prove that this is the only counter-example in Chapter 4.

A partitioning of the edges of a graph G into perfect matchings is a *1-factorisation*. A 1-factorisation is *perfect* if the union of every pair of its perfect matchings forms a Hamiltonian cycle of G. Observe that k-regular G on even number of vertices has a perfect 1-factorisation if and only if $\mathcal{M}(G)$ contains a complete graph on k vertices as a subgraph. Wanless [86] proved that $K_{p,p}$ and $K_{2p-1,2p-1}$ have perfect 1-factorisation if p is a prime and proved that $K_{n,n}$ has no perfect 1-factorisation if n is even and $n > 2$. Wanless [86] conjectured that $K_{n,n}$ has a perfect 1-factorisation if n is odd and $n \geq 3$.

We proved [37] that if n is even or $n = 1$, then $\mathcal{M}(K_{n,n})$ is connected and bipartite, otherwise $\mathcal{M}(K_{n,n})$ is not bipartite and it has two components. We [37] also proved that the distance between every pair of perfect matchings in $\mathcal{M}(K_{n,n})$ is at most 3. Moreover, we [37] computed exact distance between every pair of perfect matching in $\mathcal{M}(K_{n,n})$

Chapter 3

Perfect matchings extend to Hamiltonian cycles

In this chapter we present the proof of Kreweras' [59] conjecture 2.1 which was published in the paper [35].

Let us consider a perfect matching P of the hypercube Q_d which is contained in a Hamiltonian cycle C of Q_d. Let R denote the set of edges contained in the cycle C but not in P. Obviously, R is also a perfect matching of Q_d. Hence, Kreweras' conjecture can be restated in the following way:

For every perfect matching P of the hypercube Q_d, $d \geq 2$, there exists a perfect matching R such that $P \cup R$ is a Hamiltonian cycle of Q_d.

In fact, we prove the following theorem which is clearly stronger than the above and so implies Kreweras' conjecture.

Theorem 3.1. *For every perfect matching P of $K(Q_d)$ there exists a perfect matching R of Q_d, $d \geq 2$, such that $P \cup R$ is a Hamiltonian cycle of $K(Q_d)$.*

The crucial step of our proof lies in the following lemma. A forest is *linear*, if each component of it is a path.

Lemma 3.2. *Let P be a matching of $K(Q_d)$ that is not perfect. Then, there exists a perfect matching R of Q_d, $d \geq 2$, such that $P \cap R = \emptyset$ and $P \cup R$ is a linear forest.*

Before proof the lemma, let us first prove the theorem.

Proof of Theorem 3.1. Let $e = xy$ be an arbitrary edge of P. For the matching $P' = P \setminus \{e\}$, by Lemma, there exists a perfect matching R of Q_d such that $P' \cap R = \emptyset$ and $P' \cup R$ is a linear forest. If $e \in R$ then every vertex of the graph with edge set $(P' \cup R) \setminus \{e\}$ has even degree, but $P' \cup R$ is a forest. Hence, $e \notin R$. Now, it easily follows that $P' \cup R$ is a Hamiltonian path of $K(Q_d)$ from x to y. Hence, $P \cup R$ is a Hamiltonian cycle of $K(Q_d)$. □

Now, we prove the lemma:

Proof of Lemma 3.2. The proof proceeds by induction on d. The statement holds for $d = 2$. Let us suppose that the statement is true for every hypercube Q_k with $2 \leq k \leq d - 1$ and let us prove it for d.

We know that P is a matching which is not perfect. Hence, there must exist at least two vertices $u_1, u_2 \in V(Q_d)$ uncovered by P. We can divide the d-dimensional hypercube Q_d into two $(d-1)$-dimensional sub-hypercubes Q^1 and Q^2 such that $u_i \in V(Q^i)$ for $i \in \{1, 2\}$. Let $K^i = (V(Q^i), \binom{V(Q^i)}{2})$ and $P^i = P \cap E(K^i)$ for $i \in \{1, 2\}$.

The set of edges P^1 is a matching of K^1 which is not perfect since u_1 is not covered. Hence, there exists a perfect matching R^1 of Q^1 such that $R^1 \cap P^1 = \emptyset$ and $R^1 \cup P^1$ is a linear forest.

We would like to find a similar perfect matching R^2 of Q^2, that would join the perfect matching $R = R^1 \cup R^2$ of Q_d. However, we forbid some edges to be contained in R^2 which will preserve that $P \cup R$ is acyclic. The forbidden set of edges is

$$S = \left\{ xy \in E(K^2) \,\middle|\, \begin{array}{c} \exists x', y' \in V(Q^1) \text{ such that } xx', yy' \in P \\ \text{and there exists a path from } x' \text{ to } y' \text{ of } P^1 \cup R^1 \end{array} \right\}.$$

Every vertex v of the graph $(V(K^1), P^1 \cup R^1)$ has degree one, if and only if v is not covered by P^1. If there exists a path from x' to y' of $P^1 \cup R^1$ and $xx', yy' \in P$ and $xy \in E(K^2)$, then x' and y' are not covered by P^1 and x' and y' are vertices of both ends of a path of $P^1 \cup R^1$. Thus, the set of edges S is a matching of K^2. Moreover, the set of edges $P^2 \cup S$ is a matching of K^2 which is not perfect because S covers (not necessary all) vertices covered by P but not by P^2 and u_2 is not covered by P. Hence, there must exist a perfect matching R^2 of Q^2 by the induction such that $R^2 \cap (P^2 \cup S) = \emptyset$ and $R^2 \cup P^2 \cup S$ is a linear forest.

We show that the perfect matching $R = R^1 \cup R^2$ of Q_d satisfies the requirements of the lemma. For sake of contradiction, suppose that C is a cycle of $R \cup P$. Notice that C cannot belong to K^1 or to K^2. So C has edges in both K^1 and K^2. Now, we can shorten every path $xx' \cdots y'y$, such that $x, y \in V(Q^2)$, $x', y' \in V(Q^1)$, $xx', yy' \in P$ and $x' \cdots y'$ is a path of $P^1 \cup R^1$, by the edge $xy \in S$. Hence, we obtain a cycle of $R^2 \cup P^2 \cup S$, which is a contradiction. Thus, $P \cup R$ is a forest. Since every vertex in the graph $P \cup R$ has degree one or two, it is a linear forest. $\square$

An interested reader may notice that this proof also works if we exchange $K(Q_d)$ by $B(Q_d)$, where $B(Q_d)$ is the complete bipartite graph with the same color classes as G.

Chapter 4

Connectivity of matching graph

In this chapter we present the proof of Kreweras' [59] conjecture 2.3 which was published in the paper [36].

4.1 Extending with an edge

Let P be a perfect matching of $K(Q_d)$. Let $\Gamma(P)$ be the set of all perfect matchings R of Q_d such that $P \cup R$ is a Hamiltonian cycle of $K(Q_d)$. Note that if P is a perfect matching of Q_d and $R \in \Gamma(P)$, then $P \cup R$ is a Hamiltonian cycle of Q_d, so PR is an edge of $\mathcal{M}(Q_d)$.

We say that an edge uv of $K(Q_d)$ *crosses* a dimension $\alpha \in [d]$ if vertices u and v differ in dimension α, otherwise uv *avoids* α. A perfect matching P of $K(Q_d)$ crosses α if P contains an edge crossing α, otherwise P avoids α. Let I_d^α be the perfect matching of Q_d that contains all edges in dimension $\alpha \in [d]$. Observe that a perfect matching P of Q_d crosses α if and only if $P \cap I_d^\alpha \neq \emptyset$.

Proposition 4.1. *Let P be a perfect matching of $K(Q_d)$ avoiding $\beta \in [d]$ and $e \in I_d^\beta$. There exists $R \in \Gamma(P)$ containing e.*

Proof. The proof proceeds by induction on d. The statement holds for $d = 2$. Let us assume that the statement is true for every k-dimensional cube Q_k with $2 \leq k \leq d-1$ and let us prove it for d.

Clearly, P crosses some $\alpha \in [d] \setminus \{\beta\}$. We divide Q_d by dimension α into two $(d-1)$-subcubes Q^1 and Q^2 so that $e \in E(Q^1)$. Let $K^i := K(Q^i)$ and $P^i := P \cap E(K^i)$ for $i \in \{1, 2\}$.

The set of edges P^1 is a matching of K^1 which is not perfect since P crosses α. Let M be the set of vertices of K^1 that are uncovered by P^1. The size of M is even. If we divide Q^1 by dimension β, then numbers of vertices of M on both subcubes of Q^1 are even because P^1 avoids β. We choose an arbitrary perfect matching S^1 on vertices of M such that S^1 avoids β. The perfect matching $P^1 \cup S^1$ of K^1 avoids β. By induction there exists a perfect matching $R^1 \in \Gamma(P^1 \cup S^1)$ of Q^1 containing e. Let

$$S^2 := \left\{ xy \in E(K^2) \,\middle|\, \begin{array}{c} \exists x', y' \in V(Q^1) \text{ such that } xx', yy' \in P \text{ and} \\ \text{there exists a path between } x' \text{ and } y' \text{ of } P^1 \cup R^1 \end{array} \right\}. \tag{4.1}$$

Observe that $P^1 \cup R^1$ is a partition of Q^1 into vertex-disjoint paths between vertices uncovered by P^1. For every path between x' and y' of this partition there exist vertices

x and y of Q^2 such that $xx', yy' \in P$. Thus, the set of edges S^2 is a matching of K^2. Moreover, the set of edges $P^2 \cup S^2$ is a perfect matching of K^2 because S^2 covers each vertex covered by P but not by P^2. Hence, there exists a perfect matching $R^2 \in \Gamma(P^2 \cup S^2)$ of Q^2 by Theorem 3.1. Clearly, $R := R^1 \cup R^2$ is a perfect matching of Q_d containing e. Finally, $R \in \Gamma(P)$ by Lemma 4.2. □

Lemma 4.2. *Let P be a perfect matching of $K(Q_d)$ crossing some dimension $\alpha \in [d]$. Let Q_d be divided into two $(d-1)$-subcubes Q^1 and Q^2 by dimension α. Let $K^i := K(Q^i)$ and $P^i := P \cap E(K^i)$ for $i \in \{1,2\}$. Let S^1 be a perfect matching on vertices of $K(Q^1)$ uncovered by P^1. Let $R^1 \in \Gamma(P^1 \cup S^1)$. Let S^2 be given by (4.1). Let $R^2 \in \Gamma(P^2 \cup S^2)$ and $R := R^1 \cup R^2$. Then $R \in \Gamma(P)$.*

Proof. We prove that $P \cup R$ is a Hamiltonian cycle of $K(Q_d)$. Suppose on the contrary that C is a cycle of $P \cup R$ which is not Hamiltonian. Since P crosses α, both S^1 and S^2 are non-empty sets. Because $P^i \cup S^i \cup R^i$ is a Hamiltonian cycle of K^i, whole cycle C cannot belong to K^i, for $i \in \{1,2\}$. So C has edges in both K^1 and K^2. Now, we shorten every path $xx' \cdots y'y$ such that $x, y \in V(Q^2)$; $x', y' \in V(Q^1)$; $xx', yy' \in P$ and $x' \cdots y'$ is a path of $P^1 \cup R^1$ by the edge $xy \in S^2$. Hence, we obtain a cycle C' of $(P^2 \cup S^2) \cup R^2$. We prove that C' does not contain a vertex of K^2 which is a contradiction because $(P^2 \cup S^2) \cup R^2$ is a Hamiltonian cycle of K^2.

If C does not contain a vertex u of K^2, then C' also does not contain u. Suppose that C does not contain a vertex v of K^1. Let x' and y' be the end vertices of the longest path of $P^1 \cup R^1$ that contains v. Let $xx', yy' \in P$. Observe that $x, y \in V(K^2)$ and $xy \in S^2$. Hence, C' does not contain x and y. □

Observe that the perfect matching R obtained in Lemma 4.2 avoids dimension α. The interested reader may ask whether there exists a perfect matching R in Theorem 3.1 that avoids given set of dimension $A \subset [d]$. Clearly, the graph on edges of P and allowed edges of Q_d (i.e. edges of Q_d that avoid every dimension of A) must be connected. Gregor [49] proved that this is also a sufficient condition which implies following lemma.

Lemma 4.3. *For every perfect matching P of $K(Q_d)$ and $\alpha \in [d]$ there exists $R \in \Gamma(P)$ avoiding α if and only if P crosses α where $d \geq 2$.*

4.2 Bipartiteness of $\mathcal{M}(K_{n,n})$

There is a natural one-to-one correspondence between perfect matchings of the complete bipartite graph $K_{n,n}$ and permutations on a set of size n. A permutation π is *even* if $n - k$ is even where k is a number of cycles of π, otherwise π is *odd*. It is well-known that $\pi_1 \circ \pi_2$ is even if and only if permutations π_1 and π_2 have the same parity. Hence, the inverse permutation π_2^{-1} has the same parity as π_2.

Let $c(P)$ be the number of components of the graph on a set of edges P. Recall that $B(G)$ is the complete bipartite graph with the same color classes as a bipartite and connected graph G.

Let P_1 and P_2 be perfect matchings of $K_{n,n}$ and π_1 and π_2 be their corresponding permutations. Observe that $c(P_1 \cup P_2)$ is equal to the number of cycles of $\pi_1 \circ \pi_2^{-1}$. If n is even and $P_1 \cup P_2$ is a Hamiltonian cycle of $K_{n,n}$, then π_1 and π_2 have different parities. Hence, $\mathcal{M}(K_{n,n})$ is bipartite for n even. The matching graph $\mathcal{M}(Q_d)$ is also bipartite because $\mathcal{M}(Q_d)$ is a subgraph of $\mathcal{M}(B(Q_d))$ which is isomorphic to $\mathcal{M}(K_{2^{d-1},2^{d-1}})$.

The above discussion proves the following theorem.

Theorem 4.4. *The matching graphs $\mathcal{M}(Q_d)$ and $\mathcal{M}(B(Q_d))$ are bipartite.*

We did not define which perfect matchings of $B(Q_d)$ are even and odd. But we know that perfect matchings P_1 and P_2 of $B(Q_d)$ belong to the same color class of $\mathcal{M}(B(Q_d))$ if and only if $c(P_1 \cup P_2)$ is even. Hence, we fix one perfect matching of $B(Q_d)$ to be even.

Let us recall that I_d^α is the perfect matching of Q_d that contains all edges in dimension $\alpha \in [d]$. We simply count that $c(I_d^\alpha \cup I_d^\beta) = 2^{d-2}$ for every two different dimensions $\alpha, \beta \in [d]$ because the graph on edges $I_d^\alpha \cup I_d^\beta$ consists of 2^{d-2} independent cycles of size 4. Hence, perfect matchings I_d^α and I_d^β belong to the same color class of $\mathcal{M}(B(Q_d))$ for $d \geq 3$. We call a perfect matching P of $B(Q_d)$ *even* if $c(P \cup I_d^1)$ is even and otherwise *odd* where $d \geq 3$.

4.3 Walks in $\mathcal{M}(Q_d)$

We will prove that $\mathcal{M}(Q_d)$ is connected by induction on d. Therefore, we need to know how we can make a walk in $\mathcal{M}(Q_d)$ from a walk in $\mathcal{M}(Q_{d-1})$. In this section we present two lemmas which help us.

Let P^0 and P^1 be perfect matchings of Q_{d-1}. We denote by $\langle P^0|P^1\rangle$ the perfect matching of Q_d containing P^i in the $(d-1)$-subcube of vertices having i in the coordinate d for $i \in \{0,1\}$.

Lemma 4.5. *Let P_1, P_2, P_3, R_1, R_2, and R_3 be perfect matchings of Q_{d-1} such that $P_1 \cup P_2$, $P_2 \cup P_3$, $R_1 \cup R_2$, and $R_2 \cup R_3$ are Hamiltonian cycles of Q_{d-1}. If $P_2 \cap R_2 \neq \emptyset$, then there exists a perfect matching S of Q_d such that $\langle P_1|R_1\rangle \cup S$ and $S \cup \langle P_3|R_3\rangle$ are Hamiltonian cycles of Q_d. Moreover, S crosses the dimension d and every dimension that is crossed by P_2 or R_2.*

Proof. Let $uv \in P_2 \cap R_2$. Let u_i be the vertex of Q_d obtained from u by appending i into dimension d, where $i \in \{0,1\}$. Vertices v_0 and v_1 are defined similarly.

Let $S := (\langle P_2|R_2\rangle \setminus \{u_0v_0, u_1v_1\}) \cup \{u_0u_1, v_0v_1\}$. The graph on edges $\langle P_1|R_1\rangle \cup \langle P_2|R_2\rangle$ consists of two cycles covering all vertices of Q_d. These cycles are joined together in $\langle P_1|R_1\rangle \cup S$. Hence, $\langle P_1|R_1\rangle \cup S$ is a Hamiltonian cycle of Q_d. Similarly, $S \cup \langle P_3|R_3\rangle$ is a Hamiltonian cycle of Q_d.

The edge u_0u_1 crosses dimension d, so S also crosses d. Let us consider a dimension $\beta \in [d-1]$ which is crossed by P_2 or R_2. Without loss of generality we suppose that P_2 crosses β. There exist at least 2 edges crossing β in P_2. It can happen that the edge u_0v_0 is one of them, so at least one edge crossing β remains in S. □

Let P be a perfect matching of $K(Q_d)$ and $A \subseteq [d]$. We say that P *crosses* A if P crosses every dimension of A.

Lemma 4.6. *Let P_1, P_2, P_3, and R_1 be perfect matchings of Q_{d-1} such that $P_1 \cup P_2$ and $P_2 \cup P_3$ are Hamiltonian cycles of Q_{d-1}. Let $\alpha, \beta \in [d-1]$, $\alpha \neq \beta$. If P_2 crosses $[d-1] \setminus \{\alpha\}$ and R_1 avoids β, then there exists a perfect matching S of Q_d such that $\langle P_1|R_1\rangle \cup S$ and $S \cup \langle P_3|R_1\rangle$ are Hamiltonian cycles of Q_d and S crosses $[d] \setminus \{\alpha\}$.*

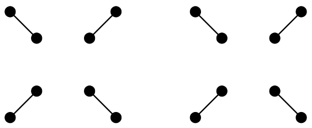
Proof. Let $e \in P_2 \cap I_{d-1}^\beta$. There exists $R_2 \in \Gamma(R_1)$ containing e by Proposition 4.1. If we apply Lemma 4.5 on P_1, P_2, P_3, R_1, R_2, and R_1, then we obtain a perfect matching S which satisfies the requirements of this lemma. □

4.4 Base of induction

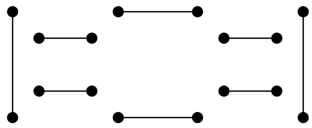
Let us recall that M_d is obtained from $\mathcal{M}(Q_d)$ by contracting all vertices of $\mathcal{M}(Q_d)$ whose corresponding perfect matchings are isomorphic. Let P and R be perfect matchings of Q_d. If there exists a walk between vertices representing P and R in $\mathcal{M}(Q_d)$, then the length of the shortest one is $d(P,R)$, otherwise $d(P,R)$ is infinity. Hence, $d(P,R) < \infty$ means that P and R belong to the same component of $\mathcal{M}(Q_d)$.

The proof, that $\mathcal{M}(Q_d)$ is connected, proceeds by induction on d. We present a base of this induction in this section. We showed that $\mathcal{M}(Q_3)$ has 3 components (see Figure 2.1), so the induction starts from $d = 4$. Kreweras [59] proved that M_4 is connected (see Figure 2.2). We prove that if M_d is connected and $d \geq 4$, then $\mathcal{M}(Q_d)$ is connected. Hence, $\mathcal{M}(Q_4)$ is connected.

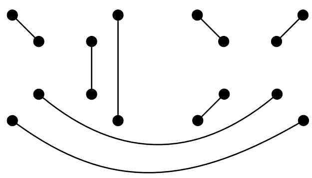
First, we present a simple lemma.



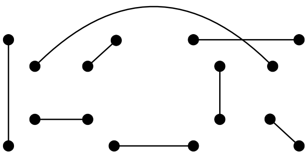
Perfect matching $S_4^0 = I_4^\alpha$



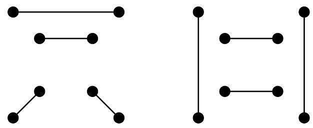
Perfect matching S_4^1



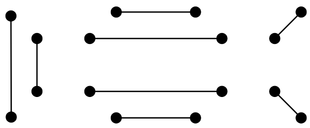
Perfect matching S_4^2



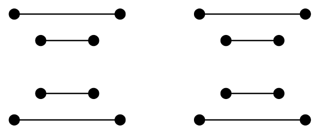
Perfect matching S_4^3



Perfect matching S_4^4



Perfect matching S_4^5



Perfect matching $S_4^6 = I_4^\beta$

Figure 4.1: The walk between perfect matchings I_4^α and I_4^β in $\mathcal{M}(Q_4)$.

Lemma 4.7. *If $d \geq 4$, then $d(I_d^\alpha, I_d^\beta) \leq 6$ for every $\alpha, \beta \in [d]$, $\alpha \neq \beta$.*

Proof. The proof proceeds by induction on d. The walk between I_4^α and I_4^β is drawn in Figure 4.1.

Let

$$I_{d-1}^\alpha = S_{d-1}^0, S_{d-1}^1, S_{d-1}^2, S_{d-1}^3, S_{d-1}^4, S_{d-1}^5, S_{d-1}^6 = I_{d-1}^\beta$$

be a walk in $\mathcal{M}(Q_{d-1})$. Let $S_d^i := \left\langle S_{d-1}^i | S_{d-1}^i \right\rangle$ for even i. For odd i let S_d^i be given by Lemma 4.5 where $P_1 = R_1 := S_{d-1}^{i-1}$, $P_2 = R_2 := S_{d-1}^i$, and $P_3 = R_3 := S_{d-1}^{i+1}$. Then

$$I_d^\alpha = S_d^0, S_d^1, S_d^2, S_d^3, S_d^4, S_d^5, S_d^6 = I_d^\beta$$

is a walk in $\mathcal{M}(Q_d)$. $\square$

Let us recall that perfect matchings P and R are isomorphic if there exists an isomorphism $f : V(Q_d) \to V(Q_d)$ such that $f(u)f(v) \in R$ for edge $uv \in P$. This relation of isomorphism is an equivalence on the set of all perfect matching. Let $[P]$ be the equivalence class containing P. Observe that $[I_d] := \{I_d^\alpha \mid \alpha \in [d]\}$ is an equivalence class. If there exists a walk between $[P]$ and $[R]$ of M_d, then the length of the shortest one is $d([P],[R])$, otherwise $d([P],[R])$ is infinity.

Let us consider perfect matchings P and R of Q_d such that $d([P],[R]) = 1$. There exist isomorphisms f and g such that $f(P) \cup g(R)$ forms a Hamiltonian cycle. Moreover, $P \cup f^{-1}(g(R))$ forms a Hamiltonian cycle. Hence, we have a perfect matching $f^{-1}(g(R)) \in \Gamma(P)$ such that $f^{-1}(g(R))$ is isomorphic to R.

Proposition 4.8. *If $d \geq 4$ and M_d is connected, then $\mathcal{M}(Q_d)$ is connected.*

Proof. We prove that vertices $\{P \in V(\mathcal{M}(Q_d)) \mid [P][I_d] \leq k\}$ belong into one component of $\mathcal{M}(Q_d)$ by induction on k. This claim holds for $k = 0$ by Lemma 4.7.

Let P be a perfect matching of Q_d such that $d([P],[I_d]) = k$. There exists a perfect matching R of Q_d such that $d([R][I_d]) = k - 1$ and $d([P][R]) = 1$. Hence, there exists $R' \in \Gamma(P)$ isomorphic to R. By induction $d(I_d, R') < \infty$. Therefore, $d(P, I_d) < \infty$. □

4.5 Induction step

We define a set of perfect matchings $\mathcal{Z}(d,k,\alpha)$ of Q_d by following induction on d, where $d \geq k \geq 3$ and $\alpha \in [d]$.

Definition 4.9. Let $\mathcal{Z}(d,d,\alpha)$ contain only I_d^α. The set $\mathcal{Z}(d,k,\alpha)$, where $d > k \geq 3$ and $\alpha \in [d]$, is the set of all perfect matchings of Q_d in the form $\langle P_1|P_2\rangle$, where $P_1 \in \mathcal{Z}(d-1,k,\alpha)$ and P_2 is an even perfect matching of Q_{d-1} avoiding some dimension $\beta \in [d] \setminus \{\alpha\}$.

Observe that every perfect matching of $\mathcal{Z}(d,k,\alpha)$ is even and it contains I_k^α in some k-subcube Q_k. We want to prove that the graph $\mathcal{M}(Q_d)$ is connected, so we need to show that there exists a perfect matching I of Q_d such that for every perfect matching P of Q_d there exists a walk between P and I in $\mathcal{M}(Q_d)$. Lemma 4.7 says that perfect matchings $[I_d]$ belong to a common component of $\mathcal{M}(Q_d)$, so it is sufficient to find a walk from P to an arbitrary one of $[I_d]$. Without loss of generality we assume that P is odd by Theorems 3.1 and 4.4. We find this walk in two steps: First, we find a walk from P to some perfect matching of $\mathcal{Z}(d,k,\alpha)$ for some $\alpha \in [d]$ and k, $d \geq k \geq 3$. Next, for every perfect matching of $\mathcal{Z}(d,k,\alpha)$ we find a walk to some perfect matching of $\mathcal{Z}(d,k+1,\alpha)$, so by induction on k we obtain a walk from P to $\mathcal{Z}(d,d,\alpha)$ which contains only I_d^α by definition.

Since Q_d is bipartite, we call vertices of one color class *black* and the other *white*.

Lemma 4.10. *For every odd perfect matching P of $B(Q_d)$ there exists $Y \in \mathcal{Z}(d,k,\alpha)$ for some dimension $\alpha \in [d]$ and k, $d \geq k \geq 3$, such that $d(P,Y) \leq 3$.*

Proof. We prove by induction on d that for every perfect matching P of $B(Q_d)$ there exist perfect matchings R, X and Y of Q_d such that $P \cup R, R \cup X$ and $X \cup Y$ are Hamiltonian cycles and X crosses $[d] \setminus \{\alpha\}$ and $Y \in \mathcal{Z}(d,k,\alpha)$.

First, we prove the statement for $d = 3$. Let P be an odd perfect matching of $B(Q_3)$. Therefore, $c(P \cup I_3^\delta)$ is 1 or 3 for every $\delta \in [3]$. If there exists $\delta \in [3]$ such that $c(P \cup I_3^\delta) = 1$, then we choose $R := Y := I_3^\delta$ and $X \in \Gamma(R)$.

We prove that there exists $\delta \in [3]$ such that $c(P \cup I_3^\delta) = 1$. Suppose on the contrary that $c(P \cup I_3^\delta) = 3$ for every $\delta \in [3]$. The graph on edges $P \cup I_3^\delta$ consists of two common edges and one cycle of size 4. Perfect matchings of $[I_3]$ are pairwise disjoint and P has two common edges with each of them. This is a contradiction because P has only 4 edges.

In the induction step we need to have a dimension $\gamma \in [d]$ that is crossed by at least 4 edges of P. If $d \geq 5$, such a dimension exists for every perfect matching P of $B(Q_d)$ by the pigeonhole principle. Every perfect matching P of $B(Q_4)$ has 8 edges. If P contains an edge crossing at least two dimensions, then we use the pigeonhole principle again.

A perfect matching P of Q_4 is *balanced* if it has 2 edges in every dimension. Luckily, Kreweras [59] proved that there are 8 perfect matchings of Q_4 up to isomorphism and only two of them are balanced; see Figure 2.2. Check that the balanced perfect matchings S_4^3 drawn in Figure 4.1 and R^1 drawn of Figure 4.2 satisfy the requirements of this lemma.

Now, we present the induction step. Let $\gamma \in [d]$ such that P has at least 4 edges crossing γ. Without loss of generality we assume that $\gamma = d$. We divide Q_d into two $(d-1)$-subcubes Q^1 and Q^2 by dimension γ. Let $B^i := B(Q^i)$ and $P^i := P \cap E(B^i)$ for $i \in \{1, 2\}$. Let M be the set of vertices of B^1 that are uncovered by P^1. We know that $|M| \geq 4$. Moreover, M has the same number of black vertices as white ones.

Let b_1 and b_2 be two different black vertices of M and w_1 and w_2 be two different white vertices of M. Let S' be a matching of B^1 covering $M \setminus \{b_1, b_2, w_1, w_2\}$. We have two ways of extending S' to obtain a matching S^1 of B^1 covering M: We can insert edges $\{b_1w_1, b_2w_2\}$ or $\{b_1w_2, b_2w_1\}$. Those two ways give us two perfect matchings $P^1 \cup S^1$ of B^1 having different parity. Of course, we choose the way that gives us odd perfect matching $P^1 \cup S^1$.

Let R^1, X^1 and Y^1 be perfect matchings of Q^1 given by induction – $(P^1 \cup S^1) \cup R^1$, $R^1 \cup X^1$ and $X^1 \cup Y^1$ are Hamiltonian cycles of B^1, X^1 crosses $[d] \setminus \{\alpha\}$ and $Y^1 \in \mathcal{Z}(d-1, k, \alpha)$. Hence, R^1 is even by Theorem 4.4. Let S^2 be given by (4.1).

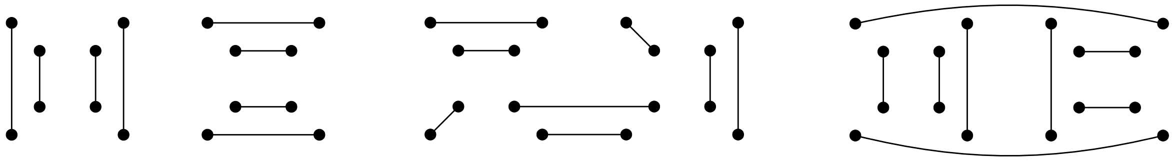
We prove that $P^2 \cup S^2$ is odd. Let $\bar{R}^2 \in \Gamma(P^2 \cup S^2)$ by Theorem 3.1. Let $\bar{R} := R^1 \cup \bar{R}^2$. By Lemma 4.2 it holds that $\bar{R} \in \Gamma(P)$, so $\bar{R}$ is even by Theorem 4.4. Also $\bar{R}^2$ is even because R^1 and $\bar{R}$ are even. Hence, $P^2 \cup S^2$ is odd by Theorem 4.4. Moreover, $P^2 \cup S^2 \neq I_{d-1}^\alpha$.

Hence, the perfect matching $P^2 \cup S^2$ crosses some $\beta \in [d] \setminus \{\alpha\}$ and there exists $R^2 \in \Gamma(P^2 \cup S^2)$ avoiding β by Lemma 4.3. Let $R := R^1 \cup R^2$. Therefore, $R \in \Gamma(P)$ by Lemma 4.2 and R is even by Theorem 4.4. Because R^1 is even, R^2 is even. We apply Lemma 4.6 on R^1, X^1, Y^1 and R^2 to obtain a perfect matching X such that $\langle R^1 | R^2 \rangle \cup X$ and $X \cup \langle Y^1 | R^2 \rangle$ are Hamiltonian cycles of Q_d and X crosses $[d] \setminus \{\alpha\}$. Finally, $Y := \langle Y^1 | R^2 \rangle \in \mathcal{Z}(d, k, \alpha)$ by definition. □

Lemma 4.11. *Let $P \in \mathcal{Z}(d, k, \alpha)$, where $3 \leq k < d$ and $\alpha \in [d]$. If $\mathcal{M}(Q_k)$ is connected or $k = 3$, then there exists $S \in \mathcal{Z}(d, k+1, \alpha)$ such that $d(P, S) < \infty$.*

Proof. We prove by induction on d that for every $P \in \mathcal{Z}(d, k, \alpha)$ there exists a walk $P = R_0, R_1, \ldots, R_n = S$ in $\mathcal{M}(Q_d)$ of even length such that R_l crosses $[d] \setminus \{\alpha\}$ for every odd l and $S \in \mathcal{Z}(d, k+1, \alpha)$. The base of this induction is for $d = k + 1$.

By definition of $\mathcal{Z}(d, k, \alpha)$ we divide P into perfect matchings P^1 and P^2 such that $P = \langle P^1 | P^2 \rangle$, $P^1 \in \mathcal{Z}(d-1, k, \alpha)$ and P^2 is an even perfect matching of Q_{d-1} avoiding some $\beta \in [d] \setminus \{\alpha\}$.



Perfect matching $R_0 = P = [I_3^\alpha | I_3^\gamma]$ Perfect matching R_1 Perfect matching R_2

Perfect matching R_3 Perfect matching $R_4 = I_4^\alpha = S$

Figure 4.2: A walk between $P \in \mathcal{Z}(4,3,\alpha)$ and I_4^α.

First, we present the base of induction for $d = 4$, so $k = 3$. By definition, $P^1 = I_3^\alpha$ and P^2 is even. There are two perfect matchings of Q_3 up to isomorphism with different parities; see Figure 2.1. Hence, $P^2 = I_3^\gamma$ for some $\gamma \in [3]$. If $P^2 = I_3^\alpha$, then $P = I_4^\alpha$, which belongs to $\mathcal{Z}(4,4,\alpha)$ by definition. Otherwise, the walk in Figure 4.2 satisfies requirements of this lemma.

Now, we present the base of the induction for $k \geq 4$ and $k+1 = d$. In that case $P^1 = I_k^\alpha$. There exists a walk $P^2 = R_0, R_1, \ldots, R_n = I_k^\alpha$ on $\mathcal{M}(Q_k)$ of even length because $\mathcal{M}(Q_k)$ is connected and bipartite and P^2 is even. Let $R_l' := \langle P^1 | R_l \rangle$ for even l. Clearly, $R_n' \in \mathcal{Z}(d, k+1, \alpha)$ because $R_n' = I_{k+1}^\alpha$.

Let l be odd. Since R_l is odd, it holds that $R_l \neq I_k^\alpha$. We choose an edge $e_l \in R_l \setminus I_k^\alpha$. By Proposition 4.1 there exists $Z_l \in \Gamma(I_k^\alpha)$ containing e_l. The perfect matching Z_l crosses $[k] \setminus \{\alpha\}$ by Lemma 4.3. We apply Lemma 4.5 on $R_{l-1}, R_l, R_{l+1}, I_k^\alpha, Z_l$, and I_k^α to obtain a perfect matching R_l'. The walk $P = R_0', R_1', \ldots, R_n' = I_{k+1}^\alpha$ satisfies the requirements.

Finally, we present the induction step for $k \geq 3$ and $k+1 < d$. By induction there exists a walk $P^1 = R_0, R_1, \ldots, R_n = S^1$ in $\mathcal{M}(Q_{d-1})$ of even length such that $S^1 \in \mathcal{Z}(d-1, k+1, \alpha)$ and R_l crosses $[d-1] \setminus \{\alpha\}$ for every odd l. Let $R_l' := \langle R_l | P^2 \rangle$ for even l. For odd l we apply Lemma 4.6 on R_{l-1}, R_l, R_{l+1} and P^2 to obtain a perfect matching R_l' of Q_d crossing $[d] \setminus \{\alpha\}$. Now, the walk $P = R_0', R_1', \ldots, R_n' = S$ satisfies the requirements and $S \in \mathcal{Z}(d, k+1, \alpha)$. $\square$

Corollary 4.12. *Let $P \in \mathcal{Z}(d,k,\alpha)$, where $3 \leq k \leq d$ and $\alpha \in [d]$. If $\mathcal{M}(Q_l)$ is connected for every $l \in \{4, 5, \ldots, d-1\}$, then $d(P, I_d^\alpha) < \infty$.*

Proof. The proof proceeds by induction on $d - k$. If $d = k$, then $P = I_d^\alpha$ by definition of $\mathcal{Z}(d,k,\alpha)$. Let $3 \leq k < d$. By Lemma 4.11 there exists $S \in \mathcal{Z}(d, k+1, \alpha)$ such that $d(P, S) < \infty$. By induction $d(S, I_d^\alpha) < \infty$. Hence, $d(P, I_d^\alpha) < \infty$. $\square$

Theorem 4.13. *The matching graph $\mathcal{M}(Q_d)$ is connected for $d \geq 4$.*

Proof. The proof proceeds by induction on d. Kreweras [59] proved that the graph M_4 is connected; see Figure 2.2. Hence, the graph $\mathcal{M}(Q_4)$ is connected by Proposition 4.8 and the statement holds for $d = 4$. Let us assume that the graph $\mathcal{M}(Q_l)$ is connected for every l with $4 \leq l \leq d-1$. Let us prove that for some $\beta \in [d]$ and for every perfect matching P of Q_d it holds that $d(P, I_d^\beta) < \infty$.

If P is even, then we choose $R \in \Gamma(P)$ by Theorem 3.1 which is odd by Theorem 4.4. Otherwise, we simply consider $R := P$. By Lemma 4.10 there exists $S \in \mathcal{Z}(d, k, \alpha)$ such that $d(R, S) \leq 3$. By Corollary 4.12 it holds that $d(S, I_d^\alpha) < \infty$ and $d(I_d^\alpha, I_d^\beta) \leq 6$ by Lemma 4.7. $\square$

Corollary 4.14. *The graph M_d is connected for $d \geq 3$.*

Chapter 5

Conclusion

In this chapter we briefly present theorems which are built on results of this part of the thesis.

For the study of properties of the matching graph $\mathcal{M}(Q_d)$, one might ask which additional requirements can we pose on the extending perfect matching R in Theorem 3.1. For example, can we find R that satisfies Theorem 3.1 and contains only edges from a given list of dimensions of hypercube? A natural necessary condition says that the set D of allowed edges for R together with the prescribed matching P form a connected subgraph. The following result due to Gregor [49] shows that this condition is also sufficient in the case when D is formed by disjoint subcubes of (possibly different) dimensions. Let $K(A)$ be the complete graph on a set of vertices A.

Theorem 5.1 (Gregor [49]). *Let $A_1, \dots, A_m \subseteq V(Q_d)$, $d \geq 2$, be pairwise disjoint subcubes of nonzero dimension. Let $A = \bigcup_{i \in [m]} A_i$, $D = \bigcup_{i \in [m]} E(A_i)$ and let P be a perfect matching of $K(A)$. There exists $R \subseteq D$ such that $P \cup R$ forms a Hamiltonian cycle of $K(A)$ if and only if $P \cup D$ is connected.*

Feder and Subi [33] consider another generalisation of Theorem 3.1. They ask whether given perfect matching can be extended into a given number of disjoint cycles that span all vertices. A weak cycle in a graph is either a cycle or two parallel copies of a single edge, considered as a cycle of length two. A weak r-cycle decomposition of a graph is a collection of disjoint r weak cycles that span all the vertices of the graph.

Theorem 5.2 (Feder and Subi [33]). *Let P be a perfect matching of $K(Q_d)$ that has at least s edges of Q_d. Let $r \leq \left\lfloor \frac{s}{d} \right\rfloor$. Then Q_d has a perfect matching R such that $P \cup R$ is a weak r-cycle decomposition of $K(Q_d)$.*

Chen [16] consider any bipartite graph W_n obtained by adding some edges into Q_n. Note that W_n is a spanning subgraph of $B(Q_n)$ containing all edges of Q_n. Let S and T be two sets of k vertices in different color classes of Q_n. A set of vertex-disjoint paths $P_1, \dots, P_k$ of W_n covering all vertices of Q_n are called (P, T)-paths if every path P_i has one end-vertex in P and the other one in T.

Theorem 5.3 (Chen [16]). *Let W_n be any bipartite graph obtained by adding some edges into Q_n and let S and T be two sets of k vertices in different color classes of Q_n. The graph W_n has (P, T)-paths if and only if $k = 2^{n-1}$ or the graph $W_n - (S \cup T)$ has a perfect matching. Moreover, if the graph $W_n - (S \cup T)$ has a perfect matching M, then W_n has (S, T)-paths containing M.*

The proof is straightforward. Given (S,T)-paths can be decomposed into a perfect matching of $W_n - (S \cup T)$ and a perfect matching of W_n. Given perfect matching M of $W_n - (S \cup T)$ can be extended into a perfect matching M' of $K(Q_n)$. By Theorem 3.1 there exists a perfect matching R of Q_n such that $M' \cup R$ forms a Hamiltonian cycle of $K(Q_n)$. We observe that $M \cup R$ forms required (S,T)-paths of W_n.

Azarija, Gregor and Škrekovski [5] asked whether a perfect matching P of Q_n can be extended into a Hamiltonian path between given vertices x and y. Let weight $w(u)$ of a vertex u of Q_n be the number of 1's in u and weight $w(uv)$ of edge uv be $\min\{w(u), w(v)\}$. A parity of vertex u is parity of $w(u)$ and parity of edge is parity of $w(uv)$. A layer is a set of edges between two $(n-1)$-dimensional subcubes of Q_n. An odd (even) half-layer is a set of all odd (even) edges of a layer. Note that edges of Q_n are partitioned into n layers and every layer is partitioned into odd and even half-layer.

Theorem 5.4 (Azarija, Gregor and Škrekovski [5])**.** *Let x, y be vertices of opposite parity, $n \geq 5$, and let P be a perfect matching of $K(Q_n - \{x,y\})$. There exists a perfect matching R of $Q_n - \{x,y\}$ such that $P \cup R$ forms a Hamiltonian cycle of $K(Q_n - \{x,y\})$ if and only if P does not contain a half-layer of Q_n.*

The condition that P does not contain a half-layer is natural because if a Hamiltonian cycle contains 2^{n-2} edges of a half-layer, then it has to contain the same number of edges of half-layer of the opposite parity of same layer, but $Q_n - \{x,y\}$ has at most $2^{n-1} - 1$ edges of every layer.

Theorem 5.4 gives us a condition for our original question when a perfect matching P of $K(Q_n)$ can be extended into a Hamiltonian path between given vertices x and y of opposite parity. One condition is that xy is not an edge of P. Let x^P and y^P be vertices of Q_n such that xx^P and yy^P are edges of P. Let $P' = P \setminus \left\{xx^P, yy^P\right\} \cup \left\{x^P y^P\right\}$. Note that P can be extended into a Hamiltonian path between x and y by edges of Q_n if and only if P' can be extended into a Hamiltonian cycle of $K(Q_n - \{x,y\})$ by edges of Q_n. Therefore, the following theorem is equivalent to Theorem 5.4.

Theorem 5.5 (Azarija, Gregor and Škrekovski [5])**.** *Let x, y be vertices of opposite parity, $n \geq 5$, and let P be a perfect matching of $K(Q_n)$ such that $xy \notin P$. There exists a perfect matching R of $Q_n - \{x,y\}$ such that $P \cup R$ forms a Hamiltonian path between x and y if and only if $P \setminus \left\{xx^P, yy^P\right\} \cup \left\{x^P y^P\right\}$ does not contain a half-layer of Q_n.*

We say that a graph G on even number of vertices is extendable if for every perfect matching P of $K(G)$ there exists a perfect matching R of G such that $P \cup R$ forms a Hamiltonian cycle of $K(G)$ where $K(G)$ is the complete graph of vertices of G. It is easy to observe that the complete graph K_{2n} and the complete bipartite graph $K_{n,n}$ are extendable. Theorem 3.1 say that Q_d is extendable for $d \geq 2$.

Fon-Der-Flaass [44] studied minimal extendable graphs on given number of vertices. Let $E(n)$ be the minimal number of edges in an extendable graph on $2n$ vertices.

Theorem 5.6 (Fon-Der-Flaass [44])**.** $E(1) = 1$, $E(2) = 4$, $E(3) = 8$, $E(4) = 12$. *For $n \geq 4$ it holds that $3n \leq E(n) \leq 4n - 4$.*

Fon-Der-Flaass [44] conjectured that the true value of $E(n)$ is $4n - 4$. He also study which edges can be removed from Q_n to remain extendable.

Theorem 5.7 (Fon-Der-Flaass [44])**.** *If F is a set of edges of Q_n such that every 4-dimensional subcube of Q_n has at most one edge in F, then $Q_n - F$ is extendable, where $n \geq 4$.*

Part IV

Long paths and cycles in faulty hypercubes

Chapter 6

Introduction

The n-dimensional hypercube Q_n is the (bipartite) graph with all binary vectors of length n as vertices and edges joining every two vertices that differ in exactly one coordinate. The bipartite classes of Q_n consist of vertices with even, respectively odd, weight, where the *weight* $|u|$ of a vertex $u \in V(Q_n) = \{0,1\}^n$ is defined as the number of 1's in u. A set $F \subseteq V(Q_n)$ in which all vertices are from the same bipartite class, is called a *monopartite* set.

Applications of the hypercube in the theory of interconnection networks inspired many questions related to its robustness. In particular, if some faulty (or busy) vertices $F \subseteq V(Q_n)$ and all incident edges are removed from Q_n, is there a path or a cycle in the remaining graph, denoted by $Q_n - F$, which covers 'almost' all vertices? And how many vertices in the worst-case can be removed?

Clearly, if F is monopartite, the length of any cycle in $Q_n - F$ cannot exceed $2^n - 2|F|$. This leads to the following definition. A cycle of length at least $2^n - 2|F|$ in $Q_n - F$ is called a *long F-free cycle in Q_n* or *long fault-free cycle*. Let $f(n)$ be the maximum integer such that $Q_n - F$ has a long F-free cycle for every set F of at most $f(n)$ vertices in Q_n.

The study of this parameter has a numerous literature. Firstly, Chan and Lee [13] showed that $f(n) \geq (n-1)/2$. Then, Yang et al. [91] improved it to $f(n) \geq n-2$, and Tseng et al. [83] to $f(n) \geq n-1$. Next, Fu [45] significantly increased it to $f(n) \geq 2n-4$ for $n \geq 3$, and Castañeda and Gotchev [12] strengthened it further to $f(n) \geq 3n-7$ for $n \geq 5$. We [41] obtained the first quadratic lower bound $f(n) \geq n^2/10 + n/2 + 1$ for $n \geq 15$ which is presented in Chapter 8.

Theorem 6.1 ([41])**.** *Let F be a set of at most $\frac{n^2}{10} + \frac{n}{2} + 1$ faulty vertices of Q_n where $n \geq 15$. Then Q_n contains a long fault-free cycle.*

On the other hand, Koubek [58] and independently Castañeda and Gotchev [12] noticed that for every $n \geq 4$ there is a set F of $\binom{n}{2} - 1$ vertices such that $Q_n - F$ contains no cycle of length at least $2^n - 2|F|$, so $f(n) \leq \binom{n}{2} - 2$. An example of a such set F consists of all but one vertex of weight 2. Indeed, since all vertices of F have even weight, any long F-free cycle in Q_n must visit all the remaining vertices of even weight. Namely, it has to visit the vertex $\mathbf{0} = (0,\ldots,0)$ and some vertex of weight 4, which is clearly impossible as they are in different 2-connected components of $Q_n - F$.

From the previous results it follows that the above upper bound is sharp for $n = 4$ [45] and for $n = 5$ [12]. It was conjectured [12] that it is sharp for all $n \geq 4$, i.e. $f(n) = \binom{n}{2} - 2$ for $n \geq 4$. We [39] proved this conjecture and its proof is presented in Chapter 12.

Theorem 6.2 ([39]). *For every set F of at most $\binom{n}{2} - 2$ vertices in Q_n and $n \geq 4$, the graph $Q_n - F$ contains a cycle of length at least $2^n - 2|F|$.*

To prove Theorem 6.2, we need to consider a modification of this problem for long paths with prescribed endvertices. Similarly as above, a path in $Q_n - F$ between vertices u and v, and of length at least $2^n - 2|F| - 2$ is called a *long F-free uv-path in Q_n* or shortly *(F, u, v)-path*. Note that in case u and v are from different bipartite classes, the length of any long F-free uv-path is at least $2^n - 2|F| - 1$. Also note that in the case when $F \cup \{u, v\}$ is monopartite, the length of any uv-path in $Q_n - F$ cannot exceed $2^n - 2|F| - 2$, and hence a long F-free uv-path has optimal length.

Fu [46] showed that $Q_n - F$ contains a long path between any two vertices if $|F| \leq n-2$ and $n \geq 3$. To improve this result for larger sets F, one needs to introduce additional conditions on the neighbors of prescribed endvertices. Kueng et al. [60] strengthened the number of tolerable faults to $|F| \leq 2n - 5$ under the condition that the minimal degree of $Q_n - F$ is at least 2. We consider much weaker condition. A vertex u is *surrounded* by F if F contains all neighbors of u. Clearly, there is no F-free path of lenght at least 2 if

$$u \text{ is surrounded by } F \cup \{v\} \text{ in } Q_n \text{ or } v \text{ is surrounded by } F \cup \{u\} \text{ in } Q_n; \tag{6.1}$$

and such triple (F, u, v) is called *blocked* in Q_n; otherwise (F, u, v) is *free* in Q_n. Thus, the triple (F, u, v) must be free for the existence of an (F, u, v)-path if $2^n - 2|F| - 2 > 1$. We [41] proved that this necessary condition is also sufficient, up to one exception in Q_4, and this proof is presented in Chapter 7.

Theorem 6.3 ([41]). *Let F be a set of at most $2n - 4$ faulty vertices of Q_n where $n \geq 2$. For every two fault-free vertices u and v, there exists a long fault-free path between u and v in Q_n if and only if both (6.1) and (6.2) does not hold.*

Let $d(u, v)$ be (Hamming) distance of vertices u and v. On Figure 6.1 we have the following configuration for $n = 4$ and $|F| = 2n - 4$:

$$\begin{gathered} \text{there are two vertices } a \text{ and } b \text{ with } d(a, b) = 4 \text{ in } Q_4 \text{ such that} \\ F \cup \{u, v, a, b\} \text{ are the all 8 vertices of one bipartite class of } Q_4. \end{gathered} \tag{6.2}$$

Observe in this configuration that every fault-free path between u and v has length at most 4 because the graph $Q_4 \setminus (F \cup \{u, v\})$ has two components and no fault-free path between u and v can visit both components. Hence, there is no (F, u, v)-path although $|F| \leq 2n - 4$ and (F, u, v) is free. Note that there are two non-isomorphic exceptional configurations since $d(u, v)$ can be 2 or 4.

Moreover, observe that the inequality $|F| \leq 2n - 4$ in Theorem 6.3 is tight for every $n \geq 4$. On Figure 6.2 we can see three configurations of $2n - 3$ faulty vertices and two fault-free vertices u and v in Q_n such that (F, u, v) is free. Clearly, in all these configurations there is only one fault-free path between u and v of length 1 or 2, which is not long.

Note that for $|F| \leq n-2$, the right side of the equivalence in Theorem 6.3 is always satisfied. Hence, we obtain the following direct corollary.

Corollary 6.4 (Fu [46]). *For every set F of at most $n - 2$ vertices of Q_n and $n \geq 2$, there is a long F-free uv-path in Q_n between every two vertices u and v of $Q_n - F$.*

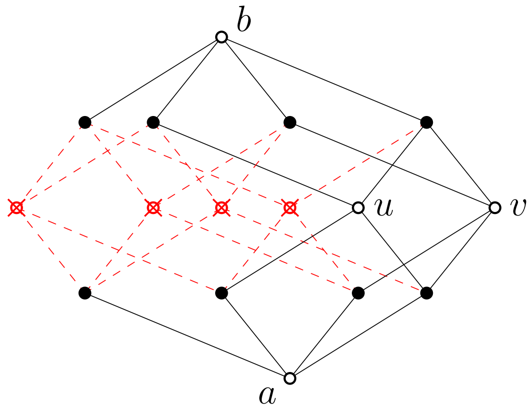


Figure 6.1: The exceptional configuration (6.2) in Q_4. The crossed points represent the faulty vertices and u, v are the prescribed endvertices for a requested long fault-free path.

We also consider a stronger condition on neighbors of endvertices to increase the number of faulty vertices. We [39] proved that F can be as large as $f(n+1)/2$ if both prescribed endvertices have only few neighbors in F which is presented in Chapter 11.

Theorem 6.5. *For every set F of at most $(n^2+n-4)/4$ vertices in Q_n and $n \geq 5$, the graph $Q_n - F$ contains a path of length at least $2^n - 2|F| - 2$ between every two vertices such that each of them has at most 3 neighbors in F.*

The general difficulty with quadratic bounds on $|F|$ in Theorems 6.2 and 6.5 is that the hypercube cannot be always split into subcubes so that the bounds hold in each subcube. Thus, the standard induction technique fails. We introduce up to our knowledge a new technique of so called *potentials* which allows us to effectively deal with such situations.

Furthermore, in the proof of Theorem 6.5 we need to consider the following extension of the studied problem for two paths. Assume that we have two different (but not necessarily disjoint) sets $A = \{u, v\}$ and $B = \{x, y\}$ of vertices of $Q_n - F$. A path P between a vertex of A and a vertex of B is called an *AB-path*. Its length $|P|$ is the number of edges in P. A pair P_1, P_2 of vertex-disjoint AB-paths in $Q_n - F$ is called an *F-free AB-routing in Q_n*. Moreover, it is said to be *long* if $|P_1| + |P_2| \geq 2^n - 2|F| - 3$. Note that if A and B are not disjoint, say $A \cap B = \{u = x\}$, then any long F-free AB-routing consists of the uu-path of length 0 and an vy-path of length at least $2^n - 2|F| - 3$.

Although the problem of long F-free AB-routings is perhaps interesting itself, we need only the following result, whose proof is presented in Chapter 9

Theorem 6.6 ([40])**.** *For every set F of at most $n-3$ vertices in Q_n, there exists a long F-free AB-routing in Q_n between every two different sets $A, B \subseteq V(Q_n) \setminus F$ such that $|A| = |B| = 2$ and $A \cup B$ is not monopartite, where $n \geq 4$.*

Note that by a simple parity argument it follows that the condition on $A \cup B$ not being monopartite is necessary in Theorem 6.6. Furthermore, the bound $|F| \leq n-3$ is tight. Indeed, let $F \cup \{b, c\}$ be the set of neighbors of some vertex $a \in V(Q_n)$ and $|F| = n-2$. Clearly, for $A = \{a, b\}$ and $B = \{b, c\}$, the only possible two vertex-disjoint AB-paths in $Q_n - F$ are $P_1 = (a, c)$ and $P_2 = (b)$ of length 1 and 0, respectively, but $2^n - 2|F| - 3 \geq 11$ for $n \geq 4$.

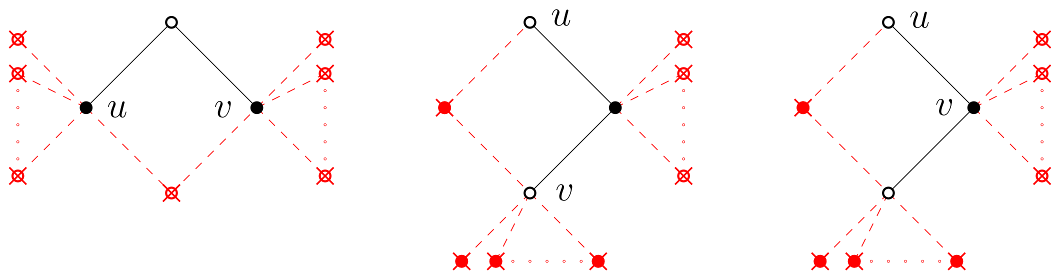


Figure 6.2: $|F| = 2n - 3$, $n \geq 4$, and (F, u, v) is free, but there is no (F, u, v)-path.

As a consequence, if $F \cup \{u, v\}$ is not monopartite, we obtain an uv-path in $Q_n - F$ of length at least $2^n - 2|F| - 1$, which is more than is guaranteed by long paths.

Corollary 6.7 ([40])**.** *For every set F of at most $n-2$ vertices of Q_n and $n \geq 4$, the graph $Q_n - F$ has an uv-path of length at least $2^n - 2|F| - 1$ for every two vertices $u, v \in V(Q_n) \setminus F$ such that $F \cup \{u, v\}$ is not monopartite.*

From Theorem 6.2 it follows that the decision problem whether the hypercube Q_n for the given set F of faulty vertices contains an F-free cycle has a trivial answer if $|F| \leq \binom{n}{2} - 2$. On the other hand, Dvořák and Koubek [26] showed that this problem is NP-hard if $|F|$ is unbounded. Moreover, they [26] presented a function $\phi(n) = \Theta(n^6)$ such that the problem remains NP-hard even if $|F| \leq \phi(n)$. Furthermore, Dvořák and Koubek [25] described a polynomial algorithm for the similar decision problem of long F-free paths between given vertices in Q_n if $|F| \leq n^2/10 + n/2 + 1$.

Those problems of long fault-free paths and cycles are sometimes considered in a more general setting also with faulty edges, not only vertices. Assume that we have f_v faulty vertices and f_e faulty edges in Q_n. A path or a cycle in Q_n is said to be *fault-free* if it contains no faulty vertex and no faulty edge. In this view, the problem of long fault-free cycles and paths is a relaxation of a substantially more difficult problem of Hamiltonian cycles and paths in hypercubes with balanced faulty vertices in the sense that in the former problem we are allowed to choose another up to f_v vertices that will be avoided (see e.g. [24] for some references on the latter problem).

As far as we know, the problem of long fault-free cycles in hypercubes was first studied by Tseng [83] who showed that such cycle in Q_n exists if $f_v + f_e \leq n - 1$, $f_v \leq n - 1$, and $f_e \leq n - 4$. This bound was slightly improved by Sengupta [81] to $f_v + f_e \leq n - 1$, and $f_v > 0$ or $f_e \leq n - 2$. Then it was substantially strengthened by Fu [45] to $f_v \leq 2n - 4$ (and $f_e = 0$), and further naturally generalized by Hsieh [52] to $f_v + f_e \leq 2n - 4$ and $f_e \leq n - 2$.

Let us also mention related results on bipancyclicity and bipanconnectivity. Tsai [82] showed that every fault-free edge and every fault-free vertex of Q_n lies on a fault-free cycle of every even length from 4 to $2^n - 2f_v$ if $f_v \leq n - 2$ (and $f_e = 0$). Ma, Liu, and Pan [68] showed that if $f_v + f_e \leq n - 2$, then Q_n contains a fault-free path of length l between every two fault-free vertices u and v for every l from $d(u, v) + 2$ to $2^n - 2f_v - 1$ such that $l - d(u, v)$ is even. There are also many results on long fault-free cycles and paths in various modifications of hypercubes, which we do not list here; see a survey of Xu and Ma [90] for further references.

Chapter 7

Long path in faulty hypercube

In this section we proof Theorem 6.3 which states that for every set F of at most $2n-4$ faulty vertices of Q_n and $n \geq 2$, there exists a path between prescribed endvertices u and v in $Q_n - F$ of length at least $2^n - 2|F| - 2$ (called (F, u, v)-path) if and only if and only if $N(u) \subsetneq F \cup \{v\}$ and $N(v) \subsetneq F \cup \{u\}$ (i.e. condition (6.1) does not hold) and the triple (F, u, v) does not form one forbiden configuration (6.2).

We prove Theorem 6.3 by induction on the dimension n. In section 7.1 we analyze surrounded vertices. In Section 7.2 we prove the base of induction by a tedious case analysis for $n \leq 4$. In Section 7.3 we prove the induction step.

7.1 Preliminaries

The main obstacle in the proof of Theorem 6.3 are vertices surrounded by faulty vertices. In the following auxiliary propositions we mainly show that there are only few such obstacles.

Proposition 7.1. *Let F be a set of at most $2n-3$ faulty vertices in Q_n where $n \geq 2$. Then, at most one vertex of Q_n is surrounded by F.*

Proof. Suppose on the contrary that two vertices u and v of Q_n are surrounded by F. Since each of them has n faulty neighbors, and they have at most 2 faulty neighbors in common, it follows that $|F| \geq 2n-2$, a contradiction. □

In the following proposition we show that at most one triple (F, u, v) is blocked when $|F| \leq 2n-4$ and the vertex u is fixed and not surrounded by F itself.

Proposition 7.2. *Let F be a set of at most $2n-4$ faulty vertices in Q_n where $n \geq 2$, and let $u \in V(Q_n)$ be not surrounded by F. Then, (F, u, v) is blocked for at most one vertex $v \in V(Q_n)$.*

Proof. First, assume that u has exactly one fault-free neighbor v. Thus, u is surrounded by $F \cup \{v\}$ and not surrounded by $F \cup \{w\}$ for any other vertex w. By Proposition 7.1, no other vertex than u is surrounded by $F \cup \{v\}$. It follows that no vertex is surrounded by $F \cup \{u\}$, so v is the only vertex such that (F, u, v) is blocked.

Now assume that u has at least 2 fault-free neighbors. Thus, u is not surrounded by $F \cup \{w\}$ for any vertex w. By Proposition 7.1, at most one vertex v is surrounded by $F \cup \{u\}$. Therefore, (F, u, v) is blocked for at most one vertex v. □

Next, we show that at most one triple (F, u, v) is blocked when $|F| \leq 2n-5$ and uv is required to be a fault-free edge. We say that an edge uv is fault-free if neither u nor v is faulty.

Proposition 7.3. *Let F be a set of at most $2n-5$ faulty vertices in Q_n where $n \geq 3$. Then, (F, u, v) is blocked for at most one fault-free edge $uv \in E(Q_n)$.*

Proof. Suppose on the contrary that triples (F, u, v) and (F, u', v') are blocked for two fault-free edges $uv, u'v' \in E(Q_n)$. Assume that u is surrounded by $F \cup \{v\}$, and u' is surrounded by $F \cup \{v'\}$. Observe that $u \neq u'$ since v and v' are fault-free. But then, both u and u' are surrounded by $F \cup \{v, v'\}$, which contradicts Proposition 7.1. □

The following proposition is useful in situations when we have a long fault-free path P in Q_L and we need to find an edge $a_L b_L$ on P such that there is a long fault-free path between a and b in Q_R.

Proposition 7.4. *Let F be a set of at most $2n-4$ faulty vertices in Q_n where $n \geq 2$. For every path P in Q_n, if P contains at least three fault-free edges uv such that (F, u, v) is blocked, then it contains a fault-free edge ab such that (F, a, b) is free.*

Proof. Let uv be a fault-free edge of P such that (F, u, v) is blocked, and both u and v are inner vertices of P. Such edge exists since only two edges of P can contain an endvertex. Assume that u is surrounded by $F \cup \{v\}$, and let w be the other neighbor of v on P. Furthermore, assume that u' is surrounded by $F \cup \{v'\}$ for some other fault-free edge $u'v'$ of P. We show that the edge vw of P is fault-free and (F, v, w) is free.

Since both u and u' have exactly $n-1$ faulty neighbors and $|F| \leq 2n-4$, they must have two faulty neighbors in common. Thus $d(u, u') = 2$ and all faulty vertices together with v (and v') belong to the same bipartite class of Q_n. Hence w is fault-free and moreover, v is not surrounded by $F \cup \{w\}$. Since u is surrounded by $F \cup \{v\}$, it follows from Proposition 7.1 that w is not surrounded by $F \cup \{v\}$. Therefore, (F, v, w) is free for a fault-free edge vw of P. □

In order to apply induction, we need to split the hypercube Q_n with up to $2n-4$ faulty vertices into two $(n-1)$-dimensional subcubes Q_L and Q_R so that both Q_L and Q_R contain at most $2n-6$ faulty vertices. This is obtained by fixing some coordinate $i \in [n]$ where $[n] = \{1, \ldots, n\}$. Formally, we define the subcube Q_L^i as the subgraph of Q_n induced by vertices that have 0 on the i-th coordinate. Similarly, the subcube Q_R^i is the subgraph of Q_n induced by vertices that have 1 on the i-th coordinate. The index i in Q_L^i and Q_R^i is omitted when it is clear or irrelevant. For $x \in V(Q_L)$, let x_R be the (only) neighbor of x in Q_R. Similarly for $x \in V(Q_R)$, let x_L be the (only) neighbor of x in Q_L.

Proposition 7.5. *Let F be a set of at most $2n-4$ vertices in Q_n where $n \geq 5$. Then Q_n can be split into Q_L and Q_R such that both subcubes contain at most $2n-6$ faulty vertices, unless $n = 5$, $|F| = 6$, and F consists of some vertex $w \in V(Q_n)$ and all his neighbors.*

Proof. If $|F| \leq 1$, we may split Q_n arbitrarily. If $2 \leq |F| \leq 2n-5$, we choose two faulty vertices and split Q_n so that they are in different subcubes. Clearly, in both these cases both Q_L and Q_R contain at most $2n-6$ faulty vertices. Now we assume that $|F| = 2n-4$.

Let A be the binary $|F| \times n$ matrix with faulty vertices in its rows. Assume that Q_n cannot be split into Q_L and Q_R such that both subcubes contain at most $2n-6$ faulty vertices. That is, each column of A contains at most one 1, or at most one 0. Without loss of generality we may assume that each column contains at most one 1. Thus A contains at most n 1's. Hence A has at most $n+1$ rows as all rows are different. Since $n+1 < 2n-4$ for $n \geq 6$, it follows that $n = 5$ and F consists of the vertex $(0, 0, \dots, 0)$ and all his neighbors. $\square$

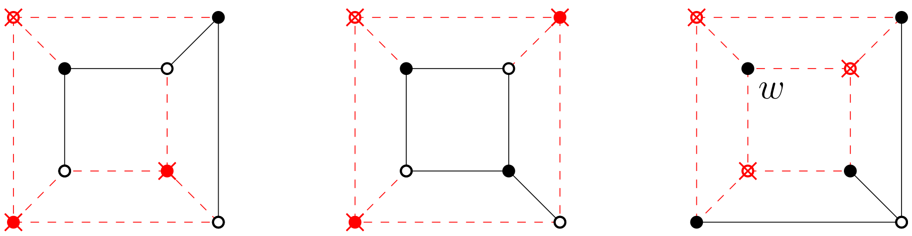
Let us recall that a path between u and v is long if it has length at least $2^n - 2|F| - 2$. We represent paths by sequences of vertices, i.e. $(u_1, u_2, \dots, u_k)$ is a path P between u_1 and u_k of length $|E(P)| = k - 1$ if all vertices $u_1, \dots, u_k$ are distinct and $u_i u_{i+1}$ is an edge for every $i \in [k-1]$. This allows us to define concatenation of paths as concatenation of their sequences. For example, if P_1 is a path between u_1 and v_1 and P_2 is a path between u_2 and v_2 such that P_1 and P_2 are vertex-disjoint and $v_1 u_2$ is an edge, then (P_1, P_2) is a path between u_1 and v_2 of length $|E(P_1)| + |E(P_2)| + 1$.

7.2 Small dimension

In this section we present the base of induction for Theorem 6.3. The case $n = 2$ is obvious since $|F| \leq 2n - 4 = 0$. For $n = 3$ we even prove a stronger statement with one additional faulty vertex than in Theorem 6.3. Namely, for $|F| \leq 2n - 3 = 3$ and every two fault-vertices u and v there exists an (F, u, v)-path if (F, u, v) is free. Note that the opposite implication does not hold since the edge uv itself (if it exists) is an (F, u, v)-path when $|F| = 3$.

Lemma 7.6. *Let F be a set of at most 3 vertices of Q_3, and let u and v be two fault-free vertices. If (F, u, v) is free, then there exists an (F, u, v)-path.*

Proof. Case 1: $|F| = 3$.



(a) (b) (c)

Figure 7.1: All configurations (up to isomorphism) of 3 faulty vertices in Q_3.

We want to find a path of length at least $2^3 - 3 \cdot 2 - 2 = 0$, so it suffices to show that u and v belong to the same component of $Q_3 \setminus F$ if (F, u, v) is free. There are tree configurations (up to isomorphism) of F with $|F| = 3$; see Figure 7.1. Observe that $Q_3 \setminus F$ on Figure 7.1(a,b) is connected. Also $Q_3 \setminus (F \cup \{w\})$ on Figure 7.1(c) is connected and w is surrounded by F. Hence the statement holds.

Case 2: $|F| = 2$.

The graph $Q_3 \setminus F$ is connected because Q_3 is 3-connected, so there exists a path P between u and v in $Q_3 \setminus F$. We want to find a fault-free path between u and v of length at least $2^3 - 2 \cdot 2 - 2 = 2$. If $d(u, v) \geq 2$, then P has this length.

Now assume that $d(u, v) = 1$. There exist two disjoint edges $x_i y_i$ such that ux_i and $y_i v$ are edges of Q_3 for $i \in \{1, 2\}$. If $x_i, y_i \notin F$ for some $i \in \{1, 2\}$, then (u, x_i, y_i, v) is a requested path. If $x_1, x_2 \in F$ or $y_1, y_2 \in F$, then (F, u, v) is blocked. It remains to find an (F, u, v)-path for the case where $F = \{x_1, y_2\}$ (or isomorphically $F = \{x_2, y_1\}$). See Figure 7.2 for such path.

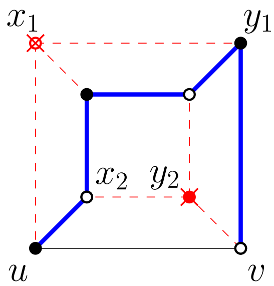


Figure 7.2: The (F, u, v)-path in Case 2 of Lemma 7.6.

Case 3: $|F| \leq 1$.

This case follows from the previous result by Fu [46] for at most $n - 2$ faulty vertices. □

Assume that Q_n is split into Q_L and Q_R. The sets of faulty vertices in Q_L and Q_R are denoted by F_L and F_R, respectively.

In Q_4 we are often in a situation when Q_4 is split into Q_L and Q_R so that $u \in V(Q_L)$ and $v \in v(Q_R)$. We would like to find a vertex x in Q_L such that there exist an (F_L, u, x)-path P_L and an (F_R, x_R, v)-path P_R and their concatenation $P = (P_L, P_R)$ is an (F, u, v)-path. Now, we present sufficient conditions on the vertex x to apply such construction.

Lemma 7.7. *Let Q_4 be split into Q_L and Q_R so that $u \in V(Q_L)$, $v \in V(Q_R)$, $|F_L| \leq 3$, $|F_R| \leq 3$ and there exists a fault-free vertex x in Q_L such that $x_R \notin F_R$, (F_R, v, x_R) is free in Q_R and at least one of the following conditions holds.*

1. *(F_L, u, x) is free in Q_L, and $d(u, x)$ or $d(v, x_R)$ is odd.*
2. *There exists a fault-free path P_L between u and x in Q_L of length at least $2^3 - 2|F_L| - 1$.*
3. *$d(u, v)$ is even, $|F_L| = 3$, and $x = u$.*

Then there exists an (F, u, v)-path in Q_4.

Proof. There exists an (F_R, x_R, v)-path P_R in Q_R by Lemma 7.6. In the first case, there exists an (F_L, u, x)-path P_L by Lemma 7.6. In the third case, let P_L be the trivial path between u and x. We show that the path $P = (P_L, P_R)$ has sufficient length in all three cases.

1. Without lost of generality we assume that $d(u, x)$ is odd. Then the length of P is $|E(P)| = |E(P_L)| + 1 + |E(P_R)| \geq 2^3 - 2|F_L| - 1 + 1 + 2^3 - 2|F_R| - 2 = 2^4 - 2|F| - 2$.
2. $|E(P)| = |E(P_L)| + 1 + |E(P_R)| \geq 2^3 - 2|F_L| - 1 + 1 + 2^3 - 2|F_R| - 2 = 2^4 - 2|F| - 2$.
3. Since $d(x_R, v)$ is odd we have $|E(P)| \geq 1 + 2^3 - 2|F_R| - 1 \geq 2^4 - 2|F| - 2$.

□

Note that if $d(u, v)$ is even, then one of $d(u, x)$ and $d(v, x_R)$ is odd for every vertex x in Q_L. Let $N(u)$, $N_L(u)$ and $N_R(u)$ be the sets of neighbors of u in Q_n, Q_L and Q_R, respectively. We conclude this section with the following lemma that serves as the basis for induction in the proof of Theorem 6.3 for $n = 4$.

Lemma 7.8. *Let F be a set of at most 4 faulty vertices in Q_4. For every two fault-free vertices u and v, there is an (F, u, v)-path if and only if (F, u, v) is free and (6.2) does not hold.*

Proof. The necessity was discussed in Section 2.

Case 1: We can split Q_4 so that $|F_L| = 4$ or $|F_R| = 4$.

Assume that $|F_L| = 4$. Let $u' = u$ if $u \in V(Q_R)$, otherwise $u' = u_R$. Similarly, let $v' = v$ if $v \in V(Q_R)$, otherwise $v' = v_R$. Clearly, there is an (F_R, u', v')-path in Q_R which is a long path in Q_4. We prolong this path by the edge uu_R if $u \in V(Q_L)$ and vv_R if $v \in V(Q_L)$ and we obtain an (F, u, v)-path in Q_4.

For the rest of the proof, we assume that $|F_L| \leq 3$ and $|F_R| \leq 3$ for every splitting of Q_4 into Q_L and Q_R, which is one of the conditions of Lemma 7.7. Furthermore, we assume that $u \in V(Q_L)$ for every splitting of Q_4, otherwise we exchange the roles of Q_L and Q_R. We distinguish the following cases.

Case 2: We can split Q_4 so that $v \in V(Q_R)$, $|F_L| = 3$ or $|F_R| = 3$, and moreover, if $d(u, v)$ is odd, then u is not surrounded by F_L in Q_L and v is not surrounded by F_R in Q_R.

Without lost of generality we assume that $|F_L| = 3$. Since $|F_R| \leq 1$, (F_R, z, v) is free in Q_R for every vertex z in Q_R. If u is surrounded by F_L in Q_L, then $d(u, v)$ is even and $u_R \notin F_R$. This configuration satisfies conditions of Lemma 7.7(c) for $x = u$. So we assume that u is not surrounded by F_L in Q_L.

Observe on Figure 7.1 that there are at least 3 vertices different from u in the component of $Q_L \setminus F_L$ containing u. Since $|F_R \cup \{v\}| \leq 2$, there is a vertex $x \in V(Q_L)$ satisfying the requirements of Lemma 7.7(b).

Case 3: We can split Q_4 so that $u, v \in V(Q_L)$, $|F_L| = 0$ and $|F_R| \leq 3$.

Observe that for every edge ab in Q_L such that $\{a, b\} \neq \{u, v\}$ there exists an (F_L, u, v)-path containing ab. Assume that $|F_R| = 3$. There exists fault-free edge ab in Q_R such that $\{a, b\} \neq \{u_R, v_R\}$ because Q_3 has 12 edges and one faulty vertex makes only 3 edges faulty. Let P_L be an (F_L, u, v)-path in Q_L containing the edge $a_L b_L$. We obtain an (F, u, v)-path from P_L by replacing the edge $a_L b_L$ with the path (a_L, a, b, b_L).

Now assume that $|F_R| \leq 2$. There exist at least 5 fault-free edges in Q_R different from $u_R v_R$ because Q_3 has 12 edges and one faulty vertex makes only 3 edges faulty. If (F_R, x, y) is blocked in Q_R for some fault-free edge xy in Q_R, then there are 2 faulty vertices in Q_R in distance 2 and there is only another one fault-free edge $x'y'$ such that (F_R, x', y') is blocked in Q_R. Hence, there exists a fault-free edge ab in Q_R different from $u_R v_R$ such that (F_R, a, b) is free in Q_R. Let P_R be an (F_R, a, b)-path in Q_R and P_L be an (F_L, u, v)-path in Q_L containing $a_L b_L$. Let P be obtained from P_L by replacing the edge $a_L b_L$ with the path P_R. Since the length of P is $|E(P_L)| - 1 + 2 + |E(P_R)| \geq 2^4 - 2|F| - 1$, it follows that P is an (F, u, v)-path.

Case 4: $d(u, v)$ is even.

We split Q_4 so that $u \in V(Q_L)$ and $v \in V(Q_R)$. If there exists splitting such that moreover $u_R \in F$ or $v_L \in F$, then we apply it. If $|F_R| = 3$ or $|F_L| = 3$, then this configuration satisfies the requirements of Case 2. So, we assume that $|F_R| \leq 2$ and $|F_L| \leq 2$.

By Proposition 7.2, there exists at most one vertex l in Q_L such that (F_L, l, u) is blocked in Q_L and at most one vertex r of Q_R such that (F_R, r, v) is blocked in Q_R. If there exists a vertex $x \in V(Q_L)$ such that $x, x_R \notin F \cup \{u, v, l, r\}$, then there exists an (F, u, v)-path by Lemma 7.7(a). When there is no such vertex x?

Note that $|F \cup \{u, v, r, l\}| \leq 8$ and Q_L has 8 vertices. There is no requested vertex x if and only if

$$\text{for every vertex } y \text{ of } Q_L \text{ exactly one of } y \text{ and } y_R \text{ belongs to } F \cup \{u, v, l, r\}. \qquad (7.1)$$

Our aim is to show that we have the exceptional configuration (6.2) if (7.1) holds. So we assume for the rest of this case that (7.1) holds. Hence $|F_L| = |F_R| = 2$ and vertices l and r exist.

We know that u is surrounded by $F_L \cup \{l\}$ in Q_L or l is surrounded by $F_L \cup \{u\}$ in Q_L. Now, we show that u is not surrounded by $F_L \cup \{l\}$ in Q_L. Suppose on the contrary that u is surrounded by $F_L \cup \{l\}$ in Q_L. If $d(u, v) = 2$, then $v_L \in N_L(u) = F_L \cup \{l\}$ which contradicts (7.1). Now, $d(u, v) = 4$. Let f be some faulty neighbor of u. It follows from (7.1) that $u_R \notin F$ and $v_L \notin F$ which contradicts our requirements on splitting because it is possible to split Q_4 by the dimension in which f and u differ. Similarly, r is not surrounded by $F_R \cup \{v\}$.

Since l is surrounded by $F_L \cup \{u\}$, vertices of $F_L \cup \{u\}$ belong to the same bipartite class A of Q_4 and l belongs to the other bipartite class B of Q_4. Let a be the only vertex of Q_L in A that does not belong to $F_L \cup \{u\}$. Similarly, the three vertices of $F_R \cup \{v\}$ belong to the same bipartite class and let b be the fourth vertex of that bipartite class in Q_R. Since u and v are in the same bipartite class A, the vertices of $F \cup \{u, v, a, b\}$ form the bipartite class A. It follows from (7.1) that $a_R = r$ and $b_L = l$. See Figure 7.3 for an illustration.

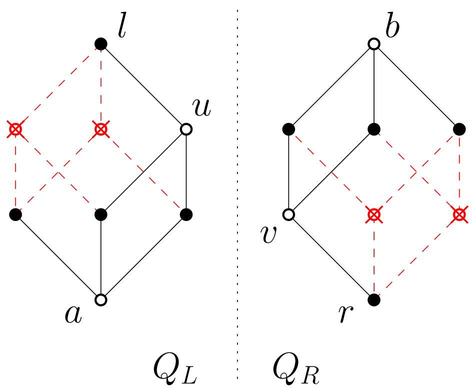


Figure 7.3: Case 4 in Lemma 7.8: the exceptional configuration (6.2).

We have $d(a, b) \geq 3$ because $a \in V(Q_L)$, $b \in V(Q_R)$, $a_R = r$, $N_R(r) = F_R \cup \{v\}$ and $b \notin F_R \cup \{v\}$. Since a and b belong to the same bipartite class, it follows that $d(a, b) = 4$. Hence, we conclude that if (7.1) holds, then we have the exceptional configuration (6.2).

Case 5: $d(u, v)$ is odd.

First, we show that we can split Q_4 so that $u \in V(Q_L)$, $v \in V(Q_R)$, u is not surrounded by F_L in Q_L, v is not surrounded by F_R in Q_R and $u_R \in F_R \cup \{v\}$.

If $d(u,v) = 1$ then we split Q_4 by the dimension in which u and v differs. Then, $u_R = v$ and the vertex u is not surrounded by F_L in Q_L and v is not surrounded by F_R in Q_R, otherwise (F,u,v) would be blocked.

Now, we assume that $d(u,v) = 3$. Let Q_A be the smallest subcube of Q_4 containing u and v. Since $d(u,v) = 3$, the dimension of Q_A is 3 and let Q_B be the complementary subcube. If there is no faulty vertex in Q_A, then we have the configuration of Case 3. If there exists a faulty vertex f in Q_A, then f is a neighbor of u or v, say u, so we split Q_4 by the dimension in which f and u differs so $u \in V(Q_L)$ and $v \in V(Q_R)$. Furthermore, u is not surrounded by F_L in Q_L, because (F,u,v) is free and $u_R = f$. If v is surrounded by F_R in Q_R, then $u_R = f$ is in $N_R(v) = F_R$ as $|F_R| \le 3$ which contradicts the assumption that $d(u,v) = 3$.

Now, Q_4 is split so that $u \in V(Q_L)$, $v \in V(Q_R)$, u is not surrounded by F_L in Q_L, v is not surrounded by F_R in Q_R and $u_R \in F_R \cup \{v\}$. If $|F_R| = 3$ or $|F_L| = 3$, then we have Case 2. So we assume that $|F_R| \le 2$ and $|F_L| \le 2$.

First, we assume that u has only one fault-free neighbor u' in Q_L. The triple (F,u',v) is free and all neighbors of u are in $F \cup \{u',v\}$. Observe on Figure 6.2 that in the exceptional configuration (6.2) there is no vertex surrounded by faulty vertices and end-vertices. Hence, the triple (F,u',v) does not form the exceptional configuration (6.2). There exists an (F,u',v)-path by Case 4 which we prolong by the edge uu' to obtain an (F,u,v)-path.

Next, we assume that v has only one fault-free neighbor in Q_R. Observe that $d(u,v) = 1$, otherwise $u_R \notin F_R \cup \{v\}$. Thus, $v_L = u$ and by exchanging the roles of Q_L and Q_R and the roles of u and v, we may proceed as in the previous paragraph. Now, both u and v have at least two fault-free neighbors in their subcubes.

Note that there is at most one faulty vertex in $N_L(u)$ and at most one faulty vertex in $N_R(u_R)$ because $u_R \in F \cup \{v\}$. By Proposition 7.2, there exists at most one vertex l in Q_L such that (F_L,u,l) is blocked in Q_L. If a vertex l exists, then there is no faulty vertex in $N_L(u)$. Hence, there is at most one vertex x in $N_L(u)$ such that $x \in F$ or (F_L,u,x) is blocked. Similarly, there is at most one vertex x in $N_L(u)$ such that $x_R \in F$ or (F_R,v,x_R) is blocked. Therefore, there exists a vertex x in $N_L(u)$ satisfying the condition of Lemma 7.7(a). □

7.3 General dimension

In this section we present the proof of our main result on long fault-free paths: Let F be a set of at most $2n-4$ faulty vertices of Q_n where $n \ge 2$. For every two fault-free vertices u and v, there exists an (F,u,v)-path in Q_n if and only if (F,u,v) is free and we do not have the exceptional configuration (6.2).

Proof of Theorem 6.3. The necessity was discussed in Section 2. We proceed by induction on n. The statement holds for $n \le 4$ by the previous section. Now we assume that $n \ge 5$ and we have two fault-free vertices u and v in Q_n such that (F,u,v) is free.

First, we consider the case when u or v has exactly one neighbor uncovered by $F \cup \{u,v\}$. Assume that u has the only neighbor u' uncovered by $F \cup \{v\}$. Clearly, the vertex v is not surrounded by $F \cup \{u'\}$. Let v' be the vertex v if v has at least two neighbors uncovered by $F \cup \{u'\}$, otherwise let v' be the only neighbor of v uncovered by $F \cup \{u'\}$. Since $|F| \le 2n-4$, the vertex u' has at least two neighbors uncovered by $F \cup \{v\}$. Moreover, if u' has exactly two such neighbors, then all faulty vertices and the vertex v are neighbors of u or u', so v has at most 3 vertices covered by $F \cup \{u'\}$, and thus $v' = v$. Hence, u' and v' have at least two neighbors uncovered by $F \cup \{u', v'\}$. Furthermore, every (F, u', v')-path avoids u (and v if $v' \neq v$), so it can be prolonged to an (F, u, v)-path. Therefore, in the following we assume that both u and v have at least two neighbors uncovered by $F \cup \{u, v\}$.

Our aim is to split Q_n into Q_L and Q_R such that $|F_L| \leq 2n - 6$ and $|F_R| \leq 2n - 6$ where $F_L = F \cap V(Q_L)$ and $F_R = F \cap V(Q_R)$. By Proposition 7.5, this can be done with the only exception when $n = 5$, $|F| = 6$, and F consists of some vertex w and all his neighbors. But when this exception happens, we may remove the vertex w from F since it cannot be visited by any path that is fault-free with respect to $F \setminus \{w\}$, so we may assume that the requested split exists.

In what follows, note that whenever we apply induction for a free triple (F', a, b) in Q_L or in Q_R, the configuration (6.2) cannot occur since $d(a, b)$ is odd or $|F'| < 2n - 6$. We assume that $u \in V(Q_L)$ and we distinguish the following cases.

Case 1: $v \in V(Q_R)$.

We may assume that $|F_L| \geq |F_R|$. Thus $|F_R| \leq n - 2$. See Figure 7.4 for an illustration.

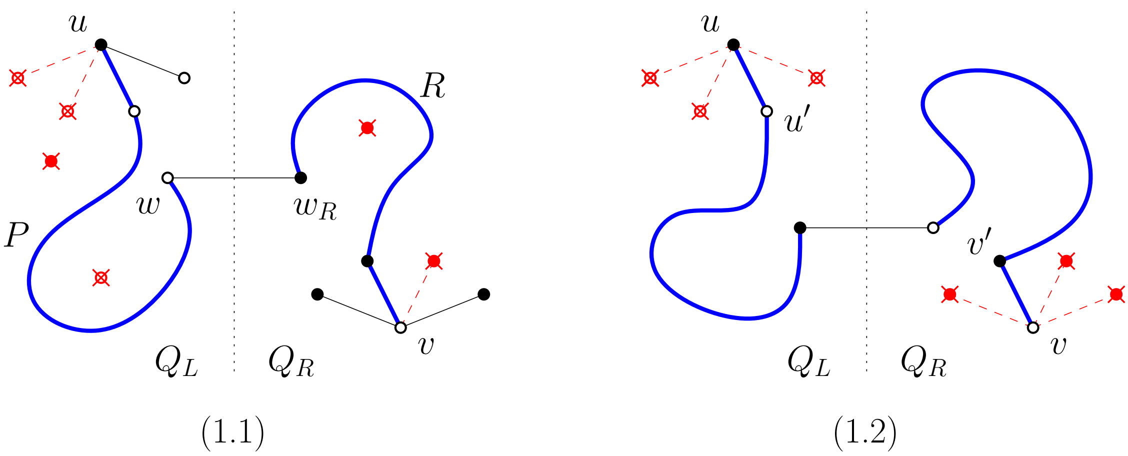


Figure 7.4: The construction of an (F, u, v)-path in Case 1 of Theorem 6.3.

Subcase 1.1: Both vertices u and v have at least 2 fault-free neighbors in their subcubes.

It follows for every $w \in V(Q_L)$ that if (F_L, u, w) is blocked in Q_L, then w is surrounded by $F_L \cup \{u\}$ in Q_L. Similarly for every $w_R \in V(Q_R)$, if (F_R, v, w_R) is blocked in Q_R, then w_R is surrounded by $F_R \cup \{v\}$ in Q_R.

We claim that there is a vertex $w \in V(Q_L)$ such that $d(u, w)$ is odd, $w_R \neq v$, both w and w_R are fault-free, (F_L, u, w) is free in Q_L, and (F_R, v, w_R) is free in Q_R. Let $A = \{w \in V(Q_L) \mid d(u, w) \text{ is odd}\}$. We say that a vertex $x \in V(Q_n)$ *eliminates* a vertex $w \in A$ if $w = x$, or $w_R = x$, or w is surrounded by $F_L \cup \{u\}$ and x is a neighbor of w, or w_R is surrounded by $F_R \cup \{v\}$ and x is a neighbor of w_R. Thus, every vertex $w \in A$ that is not eliminated by any vertex from $F \cup \{v\}$ satisfies the claim. By Proposition 7.1, at most one vertex in A is surrounded by $F_L \cup \{u\}$ in Q_L, and at most one vertex $w \in A$ has the neighbor w_R surrounded by $F_R \cup \{v\}$ in Q_R. Hence, every vertex from $F \cup \{v\}$ eliminates at most one vertex from A. Therefore the claim holds as

$$|A| - |F| - 1 \geq 2^{n-2} - 2n + 3 \geq 1 \text{ for } n \geq 5.$$

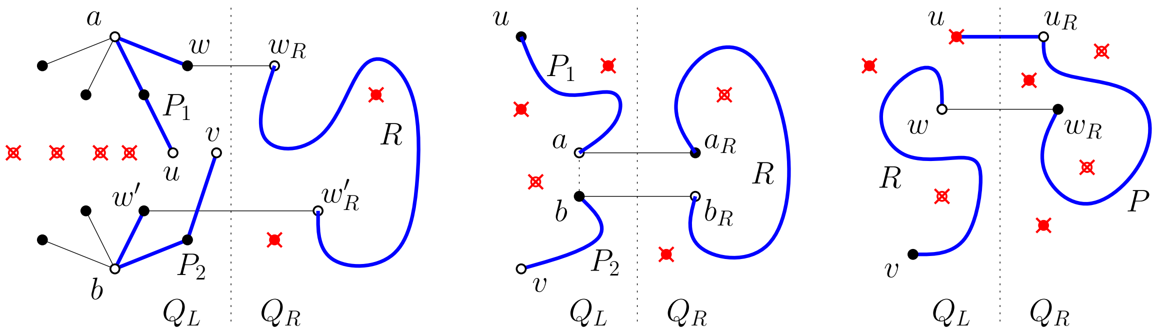
Let $w \in V(Q_L)$ be a vertex satisfying the claim above. By induction, there is an (F_L, u, w)-path P in Q_L of length at least $2^{n-1} - 2|F_L| - 1$, and an (F_R, w_R, v)-path R in Q_R. Therefore, by adding the edge ww_R we obtain an (F, u, v)-path (P, R) of length at least $2^{n-1} - 2|F_L| - 1 + 2^{n-1} - 2|F_R| - 2 + 1 = 2^n - 2|F| - 2$.

Subcase 1.2: Vertex u or v has only 1 fault-free neighbor in its subcube.

Assume that u has the only fault-free neighbor u' in Q_L. Let v' be the vertex v if v has at least two fault-free neighbors in Q_R, otherwise let v' be the only fault-free neighbor of v in Q_R. Clearly, both u' and v' have at least two fault-free neighbors in their subcubes. By the previous case, there is an (F, u', v')-path P. Then, (u, P) if $v' = v$, or (u, P, v) if $v' \neq v$, is an (F, u, v)-path.

Case 2: $v \in V(Q_L)$.

Since both u and v have at least two neighbors uncovered by $F \cup \{u, v\}$, it follows that (F_L, u, v) is free in Q_L. See Figure 7.5 for an illustration.



(2.1) (2.2) (2.3)

Figure 7.5: The construction of an (F, u, v)-path in Case 2 of Theorem 6.3.

Subcase 2.1: We have the exceptional configuration (6.2) in Q_L.

Assume that $a, b \in V(Q_L)$ are the vertices in the exceptional configuration (6.2). Let w and w' be some neighbors of a and b, respectively, such that w_R and w'_R are fault-free. Since $|F_R| \leq 2$, the triple (F_R, w_R, w'_R) is free in Q_R. Thus, by induction, there is (F_R, w_R, w'_R) path R in Q_R. Furthermore, there are disjoint fault-free paths P_1 between u and w, and P_2 between w' and v, both of length 3. Therefore, by adding the edges ww_R and $w'_R w'$ we obtain an (F, u, v)-path (P_1, R, P_2) of length at least $2^{n-1} - 2|F_R| - 2 + 2 \cdot 3 + 2 = 2^n - 2|F| - 2$.

Subcase 2.2: We do not have the exceptional configuration (6.2) in Q_L. Moreover, at least one of u_R and v_R is faulty, or $|F_R| \leq 2n - 7$, or $d(u, v)$ is odd.

Applying induction we obtain an (F_L, u, v)-path P in Q_L. We claim that there is an edge ab on P so that the edge $a_R b_R \in E(Q_R)$ is fault-free and also (F_R, a_R, b_R) is free. At most $2|F_R|$ edges $a_R b_R \in E(Q_R)$ with ab on P are faulty. However, if at least one of u_R and v_R is faulty, it is less than $2|F_R|$ edges. Furthermore, by Proposition 7.4, we may assume that (F_R, a_R, b_R) is blocked for at most 2 fault-free edges $a_R b_R \in E(Q_R)$ with ab on P, otherwise we are done. However, if $|F_R| \leq 2n - 7$, then by Proposition 7.3, (F_R, a_R, b_R) is blocked only for at most 1 fault-free edge $a_R b_R \in E(Q_R)$ with $ab \in E(P)$. Thus, some edge ab on P satisfying the claim exists as

$$\left.\begin{array}{l} E(P) - 2|F_R| - 1 \text{ for } d(u,v) \text{ even} \\ E(P) - 2|F_R| - 2 \text{ for } d(u,v) \text{ odd} \end{array}\right\} \geq 2^{n-1} - 2|F| - 3 \geq 2^{n-1} - 4n + 5 \geq 1 \text{ for } n \geq 5.$$

Hence by induction, there is an (F_R, a_R, b_R)-path R in Q_R of length at least $2^{n-1} - 2|F_R| - 1$. Therefore, by removing the edge ab and adding the edges aa_L, and $b_L b$ we obtain an (F, u, v)-path (P_1, R, P_2) of length at least

$$2^{n-1} - 2|F_L| - 2 + 2^{n-1} - 2|F_R| - 1 - 1 + 2 = 2^n - 2|F| - 2$$

where P_1 and P_2 are the subpaths of $P \setminus \{ab\}$.

Subcase 2.3: Both u_R and v_R are fault-free, $|F_R| = 2n - 6$, and $d(u, v)$ is even.

By Proposition 7.1, at most one of u_R and v_R is surrounded by F_R in Q_R. Assume that u_R is not surrounded by F_R in Q_R. We put $F'_L = F_L \cup \{u\}$, so $|F'_L| \leq 3 < 2n-6$. Note that v has at least two neighbors in Q_L that are not in F'_L since $d(u, v)$ is even. It follows for every $w \in V(Q_L)$ that if (F'_L, v, w) is blocked, then w is surrounded by $F'_L \cup \{v\}$.

We claim that there is a vertex $w \in V(Q_L)$ such that $d(v, w)$ is odd, both w and w_R are fault-free, (F'_L, v, w) is free in Q_L, and (F_R, u_R, w_R) is free in Q_R. Let $A = \{w \in V(Q_L) \mid d(u, w) \text{ is odd}\}$. By Proposition 7.2, (F_R, u_R, w'_R) is blocked for at most one vertex $w' \in A$. If that happens for some $w' \in A$, let $A' = A \setminus \{w'\}$, otherwise let $A' = A$.

We say that a vertex $x \in V(Q_n)$ *eliminates* a vertex $w \in A'$ if $w = x$, or $w_R = x$, or w is surrounded by $F'_L \cup \{v\}$ and x is a neighbor of w. Thus, every vertex $w \in A'$ that is not eliminated by any vertex from F satisfies the claim. By Proposition 7.1, at most one vertex in A is surrounded by $F'_L \cup \{v\}$. Hence every vertex from F eliminates at most one vertex from A. Therefore the claim holds as

$$|A'| - |F| \geq 2^{n-2} - 2n - 3 \geq 1 \text{ for } n \geq 5.$$

Hence by induction, there is an (F_R, u_R, w_R)-path P in Q_R of length at least $2^{n-1} - 2|F_R| - 1$. Furthermore, there is an (F'_L, w, v)-path R in Q_L that avoids u and has length at least $2^{n-1} - 2(|F_L| + 1) - 1$. Therefore, by adding the edges uu_R and $w_R w$, we obtain an (F, u, v)-path (u, P, R) of length at least

$$2^{n-1} - 2|F_R| - 1 + 2^{n-1} - 2|F_L| - 1 - 2 + 2 = 2^n - 2|F| - 2.$$

□

Chapter 8

Long cycles in faulty hypercubes

Let $D \subseteq [n]$ be a set of $d = |D|$ coordinates of Q_n. We can consider every vertex x of Q_n as a pair $x = (u, v)_D$ where $u \in \{0,1\}^{n-d}$ and $v \in \{0,1\}^d$ are projections of x on the coordinates of $[n] \setminus D$ and D, respectively. For $u \in \{0,1\}^{n-d}$ we denote by $Q_D(u)$ the d-dimensional *subcube* of Q_n induced by vertices $V_D(u) = \{(u, v)_D \mid v \in \{0,1\}^d\}$. In other words, $Q_D(u)$ is the subcube of Q_n with coordinates $[n] \setminus D$ fixed by u. The index D in $(u, v)_D$ is omitted whenever clear from the context.

Let F be a set of faulty vertices of Q_n. Recall that a cycle in Q_n is *long* if it has length at least $2^n - 2|F|$. For a set $D \subseteq [n]$ and $u \in \{0,1\}^{n-d}$ we define $F_D(u) = F \cap V_D(u)$. Assume that we want to find a long fault-free cycle in Q_n.

Our approach is based on subcube partitioning similar as in the work of Bruck et al. [11] where the hypercube is partitioned into subcubes so that each subcube contains a large fault-free component. However, instead of using the same partitioning as in [11], we apply recent results by Wiener [87] on edge multiplicity of traces in set systems which gives better bounds. We proceed as follows.

First, we find a set $D \subseteq [n]$ such that $|F_D(u)| \leq 2d - 4$ for every $u \in \{0,1\}^{n-d}$ where $d = |D|$. Then, for some Hamiltonian cycle $(u^1, u^2, \ldots, u^{2^{n-d}}, u^{2^{n-d}+1} = u^1)$ of Q_{n-d} we choose in each subcube $Q_D(u^i)$ two appropriate vertices a^i and b^i such that $a^i b^{i+1} \in E(Q_n)$ for every $i \in [2^{n-d}]$. Next, applying Theorem 6.3 we find long fault-free paths between a^i and b^i in each subcube $Q_D(u^i)$. Finally, we glue these paths together and obtain a desired long fault-free cycle in Q_n. See Figure 8.1 for an illustration.

The crucial step is the determination of the set D. Although the following theorem by Wiener [87] was originally formulated for set systems, here we take the liberty to formulate it for vertices of the hypercube.

Theorem 8.1 (Wiener [87])**.** *Let F be a set of at least $2n$ vertices of Q_n, and let $d = \left\lceil \frac{n^2}{2|F|-n-2} \right\rceil$. Then, there exists a set $D \subseteq [n]$, $|D| = d$ such that $|F_D(u)| \leq d + 1$ for every $u \in \{0,1\}^{n-d}$.*

For the choice of vertices a^i and b^i we employ the following separate lemma. Recall that a triple (F, u, v) is blocked for $F \subseteq V(Q_n)$ and $u, v \in V(Q_n)$ if u is surrounded by $F \cup \{v\}$ or v is surrounded by $F \cup \{u\}$, otherwise (F, u, v) is free.

Lemma 8.2. *Let F be a set of faulty vertices of Q_n where $n \geq 5$, and let $D \subseteq [n]$ be such that $d = |D| = 5$ and $|F_D(u)| \leq 6$ for every $u \in \{0,1\}^{n-d}$. Let $(u^1, u^2, \ldots, u^{2^{n-d}}, u^{2^{n-d}+1} = u^1)$ be a Hamiltonian cycle of Q_{n-d}. Then, there are fault-free vertices a^i and b^i in each $Q_D(u^i)$ such that*

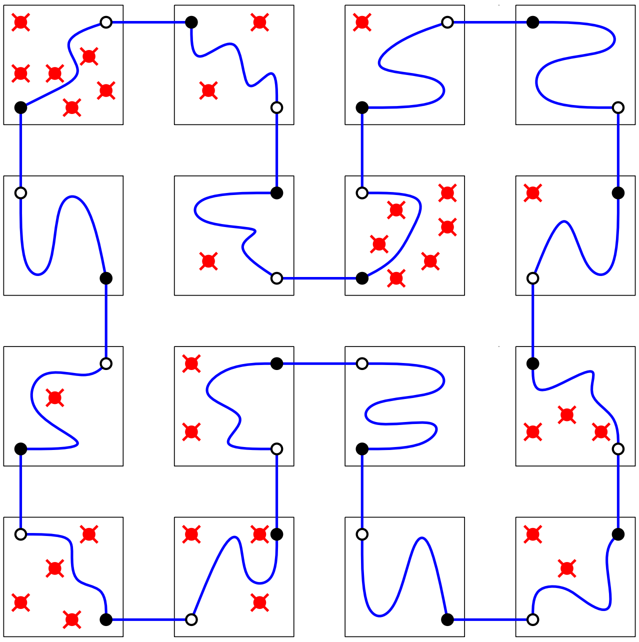


Figure 8.1: The construction of a long fault-free cycle in Theorem 6.1.

- *$d(a^i, b^i)$ is odd,*
- *$(F_D(u^i), a^i, b^i)$ is free in $Q_D(u^i)$,*
- *$a^i b^{i+1} \in E(Q_n)$ where $b^{2^{n-d}+1} = b^1$,*

for every $i \in [2^{n-d}]$.

Proof. We determine vertices a^i and b^i in this order: a^1, b^2, $a^2, \ldots, b^{2^{n-d}}$, $a^{2^{n-d}}$, $b^{2^{n-d}+1} = b^1$. Since u^i and u^{i+1} are neighbors in Q_{n-d}, every vertex in $Q_D(u^i)$ has one neighbor in $Q_D(u^{i+1})$. Let A and B be the bipartite classes of Q_n. We will choose $a^i = (u^i, v^i)$ from $A \cap V_D(u^i)$ and obtain $b^{i+1} = (u^{i+1}, v^i)$ from $B \cap V_D(u^{i+1})$. Thus $d(a^i, b^i)$ is odd and $a^i b^{i+1} \in E(Q_n)$.

There are 16 vertices in $A_i = A \cap V_D(u^i)$ since $Q_D(u^i)$ is isomorphic to Q_5. At most 6 of them are faulty since $|F_D(u^i)| \le 6$. Furthermore, at most 6 of them have faulty neighbor in $Q_D(u^{i+1})$ since $|F_D(u^{i+1})| \le 6$.

In each of the cases $i = 1$, $1 < i < 2^{n-d}$, and $i = 2^{n-d}$, we show that amongst the 4 remaining vertices of A_i, there are at most two vertices, denoted by x^i and y^i, that are not eligible for the choice of a^i.

Case $i = 1$. By Proposition 7.1, at most one vertex $x^1 \in A_1$ is surrounded by $F_D(u^1)$ in $Q_D(u^1)$. Furthermore, at most one vertex $y^1 \in A_1$ has the neighbor in $Q_D(u^2)$ surrounded by $F_D(u^2)$ in $Q_D(u^2)$.

Case $1 < i < 2^{n-d}$. By Proposition 7.2, $(F_D(u^i), x^i, b^i)$ is blocked in $Q_D(u^i)$ for at most one vertex $x^i \in A_i$. By Proposition 7.1, at most one vertex $y^i \in A_i$ has the neighbor in $Q_D(u^{i+1})$ surrounded by $F_D(u^{i+1})$ in $Q_D(u^{i+1})$.

Case $i = 2^{n-d}$. By Proposition 7.2, $(F_D(u^i), x^i, b^i)$ is blocked in $Q_D(u^i)$ for at most one vertex $x^i \in A_i$. Furthermore, at most one vertex $y^i \in A_i$ has the neighbor z in $Q_D(u^1)$ such that $(F_D(u^1), a^1, z)$ is blocked in $Q_D(u^1)$.

Hence, by choosing vertices a^i and b^i for every $i \in [2^{n-d}]$ such that

$$a^i = (u^i, v^i) \in A_i \setminus (\{x^i, y^i\} \cup F_D(u^i) \cup F_D^*(u^{i+1})) \text{ for some } v^i \in \{0,1\}^d,$$
$$b^{i+1} = (u^{i+1}, v^i) \text{ and } b^1 = b^{2^{n-d}+1},$$

where $F_D^*(u^{i+1})$ is the set of vertices of $Q_D(u^i)$ that have a faulty neighbor in $Q_D(u^{i+1})$, we obtain that both a^i and b^i are fault-free, and $(F_D(u^i), a^i, b^i)$ is free in $Q_D(u^i)$ for every $i \in [2^{n-d}]$. $\square$

Now we are ready to prove Theorem 6.1 which states that for every set F of at most $\frac{n^2}{10} + \frac{n}{2} + 1$ faulty vertices of Q_n, where $n \geq 15$, there exists contains a long fault-free cycle in Q_n

Proof of Theorem 6.1. Let $F' \supseteq F$ be some set of exactly $\left\lfloor \frac{n^2}{10} + \frac{n}{2} + 1 \right\rfloor$ vertices of Q_n. Thus $|F'| \geq 2n$ as $n \geq 15$ and by Theorem 8.1, there is a set $D \subseteq [n]$ such that $d = |D| = 5$ and $|F_D(u)| \leq |F'_D(u)| \leq 6$ for every $u \in \{0,1\}^{n-d}$. Let $(u^1, u^2, \ldots, u^{2^{n-d}}, u^{2^{n-d}+1} = u^1)$ be some Hamiltonian cycle of Q_{n-d}.

By Lemma 8.2, there are fault-free vertices a^i and b^i in each $Q_D(u^i)$ such that $d(a^i, b^i)$ is odd, $(F_D(u^i), a^i, b^i)$ is free in $Q_D(u^i)$, and $a^i b^{i+1} \in E(Q_n)$ for every $i \in [2^{n-d}]$ where $b^{2^{n-d}+1} = b^1$.

Hence by Theorem 6.3, in each $Q_D(u^i)$ there is a fault-free path P_i between b^i and a^i of length at least $2^d - 2|F_D(u^i)| - 1$. Concatenating these paths with edges $a^i b^{i+1} \in E(Q_n)$ we obtain a fault-free cycle $(P_1, P_2, \ldots, P_{2^{n-d}}, b^1)$ of length at least

$$2^{n-d} \cdot 2^d - \sum_{i \in [2^{n-d}]} 2|F_D(u^i)| - 2^{n-d} + 2^{n-d} = 2^n - 2|F|.$$

$\square$

Chapter 9

Long routing in faulty hypercubes

In this chapter we prove Theorem 6.6 and its Corollary 6.7 about long F-free routings and paths of length $2^n - 2|F| - 1$.

It is well known that Q_n contains a Hamiltonian path between every two vertices of the opposite parity. Lewinter and Widulski [62] studied the hypercube with one faulty vertex.

Proposition 9.1 (Lewinter and Widulski [62])**.** *Let $n \geq 2$ and u, v, w be distinct vertices in Q_n such that u and v have the same parity opposite to the parity of w. Then, $Q_n - \{w\}$ has a Hamiltonian uv-path.*

If F is not monopartite, then we obtain F-free path of lenght 2 more than required for long paths.

Proposition 9.2 (Hung et al. [53])**.** *Let $n \geq 4$, $F \subseteq V(Q_n)$ such that $|F| \leq n-2$ and F is not monopartite, and let $u, v \in V(Q_n) \setminus F$ be distinct vertices. Then, $Q_n - F$ has an uv-path of length at least $2^n - 2|F|$.*

In order to apply induction, we need to split the hypercube Q_n into two $(n-1)$-dimensional subcubes Q_L and Q_R. This is obtained by fixing some coordinate $i \in [n]$. Formally, we define the subcube Q_L as the subgraph of Q_n induced by vertices that have 0 on the i-th coordinate. Similarly, the subcube Q_R is the subgraph of Q_n induced by vertices that have 1 on the i-th coordinate. For a vertex x of Q_L, let x_R be the (only) neighbor of x in Q_R. Similarly for a vertex x of Q_R, let x_L be the (only) neighbor of x in Q_L.

Assume that F is a given set of faulty vertices of Q_n. The vertices of Q_n which are not in F are called *F-free*. For every $i \in [n]$ we define F_L and F_R to be the sets of faulty vertices in Q_L and Q_R, respectively.

In the following two lemmas we start with dimensions $n = 3$ and $n = 4$. Note that Lemma 9.3 is needed for Lemma 9.4, whereas Lemma 9.4 serves us as a base of induction for Theorem 6.6.

Lemma 9.3. *For every set F of at most 1 vertex of Q_3, there exists a long F-free AB-routing in Q_3 between every two disjoint sets $A, B \subseteq V(Q_3) \setminus F$ such that $|A| = |B| = 2$ and $A \cup B$ is not monopartite.*

Proof. It is trivial to verify the statement by inspection of all cases. First, consider all possible sets A, B in case $F = \emptyset$ when we search for AB-routing P_1, P_2 in Q_3 such that $|P_1| + |P_2| \geq 5$. Then, consider the case $|F| = 1$ when we need $|P_1| + |P_2| \geq 3$. $\square$

Note that the disjointness of the sets A and B is necessary in Lemma 9.3. Indeed, for $A = \{001, 110\}$, $B = \{111, 110\}$, and $F = \{000\}$, observe that there is no path between 001 and 111 in $Q_3 - \{000, 110\}$ of length at least 3, and consequently, no long F-free AB-routing in Q_3.

Lemma 9.4. *For every set F of at most 1 vertex of Q_4, there exists a long F-free AB-routing in Q_4 between every two different sets $A, B \subseteq V(Q_4) \setminus F$ such that $|A| = |B| = 2$ and $A \cup B$ is not monopartite.*

Proof. Case 1: First, we consider the case when $A = \{u, v\}$ and $B = \{x, v\}$ intersect at some vertex v. Then, we can treat v as a new faulty vertex in the set $F' = F \cup \{v\}$, so it suffices to find an ux-path in $Q_4 - F'$ of length at least $2^4 - 2|F'| - 1$. If u, x are of opposite parity, such path exists by Corollary 6.4. Now u and x are of the same parity.

If $F' = \{v\}$, then the requested ux-path exists by Proposition 9.1 since $A \cup B = \{u, x, v\}$ is not monopartite. Now we have $F' = \{f, v\}$. If f and v have opposite parity, then the requested path exists by Proposition 9.2.

Since $A \cup B$ is not monopartite, it remains to consider the case when f and v have the same parity opposite to the parity of u and x. We split Q_4 into Q_L and Q_R so that f and v are in separate subcubes, say $F'_L = \{f\}$ and $F'_R = \{v\}$, and we distinguish two subcases.

Subcase (i): If vertices u, x are in the same subcube, say $u, x \in V(Q_L)$, then from Proposition 9.1 we obtain ux-path P_L in $Q_L - F'_L$ of length 6. Let ab be an edge of P_L such that $a_R, b_R \neq v$. From Corollary 6.4 we obtain $a_R b_R$-path P_R in $Q_R - F'_R$ of length 5. After interconnecting P_R and $P_L - ab$ by edges aa_R, bb_R we get the desired ux-path in $Q_4 - F'$ of length $12 \geq 2^4 - 2|F'| - 1$.

Subcase (ii): Now vertices u, x are in different subcubes, say $x \in V(Q_L)$ and $u \in V(Q_R)$. We choose a vertex $a \in V(Q_L)$ with the opposite parity than u, $a \neq f$, and $a_R \neq u$. Note that $a \neq x$ and $a_R \neq v$. From Corollary 6.4 we obtain ax-path P_L in $Q_L - F'_L$ of length 5, and from Proposition 9.1 we obtain ua_R-path P_R in $Q_R - F'_R$ of length 6. By interconnecting these paths with the edge aa_R we obtain the desired ux-path in $Q_4 - F'$ of length $12 \geq 2^4 - 2|F'| - 1$.

Case 2: Second, we consider the case when $A = \{u, v\}$ and $B = \{x, y\}$ are disjoint. Then, we split Q_4 into Q_L and Q_R so that x, y are in different subcubes, say $x \in V(Q_L)$ and $y \in V(Q_R)$, and we distinguish two subcases depending on the vertices of A.

Subcase (i): If vertices u, v are in the same subcube, say $A \subseteq V(Q_L)$, we choose a vertex $a \in V(Q_L) \setminus F_L$ with the same parity as y, $a_R \notin F_R$, and $a \notin \{u, v, x\}$. Note that such vertex exists, since there are 4 candidate vertices in Q_L with the same parity as y, the set F blocks at most one of them, and the set $\{u, v, x\}$ blocks at most two of them, otherwise $A \cup B$ would be monopartite. For a set $B' = \{x, a\}$ it follows that A, B' are disjoint and $A \cup B'$ is not monopartite. Hence by Lemma 9.3, there is an AB'-routing P'_1, P'_2 in $Q_L - F_L$ such that $|P'_1| + |P'_2| \geq 2^3 - 2|F_L| - 3$. Assume that a is the endvertex of the path P'_1. By Corollary 6.4, there is an $a_R y$-path in $Q_R - F_R$ of length at least $2^3 - 2|F_R| - 1$ since a_R and y have opposite parity. By interconnecting P'_1 and P_R with the edge aa_R, we obtain AB-routing P_1, P'_2 in $Q_4 - F$ such that $|P_1| + |P'_2| = |P'_1| + |P_R| + 1 + |P'_2| \geq 2^4 - 2|F| - 3$.

Subcase (ii): Now vertices u, v are in different subcubes, say $u \in V(Q_L)$ and $v \in V(Q_R)$. If u and x, or v and y are of opposite parity, then from Corollary 6.4 we obtain a long F_L-free ux-path P_L in Q_L and a long F_R-free vy-path P_R in Q_R such that $|P_L| + |P_R| \geq 2^4 - 2|F| - 3$. Hence P_L, P_R is a long F-free AB-routing in Q_4.

Since $A \cup B$ is not monopartite, it remains to consider the case when u and x have the same parity opposite to the parity of v and y. We choose two vertices $a, b \in V(Q_L) \setminus F_L$ with the same parity opposite to the parity of u, and $a_R, b_R \notin F_R$. Note that such vertices exist since there are 4 candidate vertices in Q_L with the parity opposite to u and the set F blocks at most one of them. It follows that $A_L = \{u, x\}$, $B_L = \{a, b\}$ are disjoint and $A_L \cup B_L$ is not monopartite. Hence, by Lemma 9.3 there is a long F_L-free A_LB_L-routing P_1', P_2' in Q_L. Moreover, since both paths P_1', P_2' have odd length, we have $|P_1'| + |P_2'| \geq 2^3 - 2|F_L| - 2$. Assume that the A_LB_L-routing joins the vertex u with b, otherwise we switch the roles of a and b in what follows. By the definition of a, b, the sets $A_R = \{b_R, v\}$, $B_R = \{a_R, y\}$ are disjoint and $A_R \cup B_R$ is not monopartite. Hence, by Lemma 9.3 there is a long F_R-free A_RB_R-routing P_3', P_4' in Q_R. By interconnecting P_1', P_2' and P_3', P_4' with edges aa_R, bb_R we obtain AB-routing P_1, P_2 in $Q_4 - F$ such that $|P_1| + |P_2| = |P_1'| + |P_2'| + |P_3'| + |P_4'| + 2 \geq 2^4 - 2|F| - 2$. □

Now we are ready to prove Theorem 6.6, which says that for every set F of at most $n - 3$ vertices in Q_n and $n \geq 4$, there exists a long F-free AB-routing in Q_n between every two different sets $A, B \subseteq V(Q_n) \setminus F$ such that $|A| = |B| = 2$ and $A \cup B$ is not monopartite.

Proof of Theorem 6.6. We proceed by induction on the dimension n. For $n = 4$ we apply Lemma 9.4. Now assume $n \geq 5$.

First, we split Q_n into Q_L and Q_R such that we separate two arbitrarily chosen faulty vertices from F if $|F| \geq 2$, otherwise we split Q_n arbitrarily. It follows that $|F_L|, |F_R| \leq n - 4$. Thus, we may apply induction both in Q_L and Q_R. We consider the following cases.

Case 1: If both A, B are in one subcube, say $A, B \subseteq V(Q_L)$, then by induction, there is a long F_L-free AB-routing P_1', P_2' in Q_L. Let ab be an edge of P_1' or P_2', such that $a_R, b_R \notin F_R$. Such edge exists, otherwise $2^{n-1} - 2|F_L| - 3 \leq |P_1'| + |P_2'| \leq 2|F_R|$, which yields a contradiction $2^{n-1} - 3 \leq 2|F| \leq 2n - 6$ for $n \geq 5$. From Corollary 6.4 we obtain an a_Rb_R-path P_R in $Q_R - F_R$ of length $2^{n-1} - 2|F_R| - 1$ since a_R and b_R have different parity. After interconnecting P_R and P_1' or P_2' with the edges aa_R, bb_R we get the AB-routing P_1, P_2 in $Q_n - F$ such that $|P_1| + |P_2| = |P_1'| + |P_2'| + |P_R| + 1 \geq 2^n - 2|F| - 3$.

Case 2: If A is in one subcube and B in the other subcube, say $A = \{u, v\} \subseteq V(Q_L)$ and $B = \{x, y\} \subseteq V(Q_R)$, we distinguish two subcases.

Subcase (i): If u and v have different parity, then from Corollary 6.4 we obtain an uv-path P_L in $Q_L - F_L$ of length at least $2^{n-1} - 2|F_L| - 1$. Let ab be an edge of P_L such that $A' = \{a_R, b_R\}$ is disjoint with F_R and $A' \neq B$. Such edge exists, otherwise $|P_R| \leq 2|F_R| + 1$, which yields a contradiction $2^{n-1} - 2 \leq 2|F| \leq 2n - 6$ for $n \geq 5$. Since $A' \cup B$ is not monopartite, there is a long F_R-free $A'B$-routing P_1', P_2' in Q_R. By interconnecting $P_L - ab$ and P_1', P_2' with the edges aa_R, bb_R, we get an AB-routing P_1, P_2 in $Q_n - F$ such that $|P_1| + |P_2| = |P_L| + |P_1'| + |P_2'| + 1 \geq 2^n - 2|F| - 3$.

Subcase (ii): Now u and v are of the same parity. We choose vertices $B' = \{a, b\} \subseteq V(Q_L) \setminus F_L$ of the same parity opposite to the parity of u such that $A' = \{a_R, b_R\}$ is disjoint with F_R. Such vertices exists, since there are 2^{n-2} candidates in Q_L with parity opposite to the parity of u, and at most $n-3$ of them are blocked by F. Clearly, $A \neq B'$ and $A \cup B'$ is not monopartite. Thus, there is a long F_L-free AB'-routing P_1', P_2' in Q_L.

Moreover, since both P'_1, P'_2 have odd length, we have $|P'_1| + |P'_2| \geq 2^{n-1} - 2|F_L| - 2$. In the other subcube Q_R, at least one vertex of $B = \{x, y\}$ has the opposite parity to the parity of a_R, b_R, u, and v. It follows that $A' \neq B$ and $A' \cup B$ is not monopartite, and hence, there is a long F_R-free $A'B$-routing P'_3, P'_4 in Q_R. By interconnecting P'_1, P'_2 and P'_3, P'_4 with edges aa_R, bb_R we get an AB-routing P_1, P_2 such that

$$|P_1| + |P_2| = |P'_1| + |P'_2| + |P'_3| + |P'_4| + 2 \geq 2^n - 2|F| - 3.$$

Case 3: If A is one subcube, and B in both subcubes, say $A = \{u, v\} \subseteq V(Q_L)$, $x \in V(Q_L)$, $y \in V(Q_R)$, then we proceed similarly as in Case 2, Subcase (i) of Lemma 9.4. We choose a vertex $a \in V(Q_L) \setminus F_L$ with the same parity as y, $a_R \notin F_R$, and $a \notin \{u, v, x\}$. Note that such vertex exists, since there are 2^{n-2} candidate vertices in Q_L with the same parity as y, the faulty vertices block at most $n-3$ of them, the set $\{u, v, x\}$ blocks at most 3 of them, and $2^{n-2} - (n-3) - 3 \geq 1$ for $n \geq 5$. For a set $B' = \{x, a\}$ it follows that A, B' are disjoint and $A \cup B'$ is not monopartite. Hence by induction, there is an AB'-routing P'_1, P'_2 in $Q_L - F_L$ such that $|P'_1| + |P'_2| \geq 2^{n-1} - 2|F_L| - 3$. Assume that a is the endvertex of the path P'_1. By Corollary 6.4, there is an $a_R y$-path in $Q_R - F_R$ of length at least $2^{n-1} - 2|F_R| - 1$ since a_R and y have opposite parity. By interconnecting P'_1 and P_R with the edge aa_R, we obtain AB-routing P_1, P'_2 in $Q_n - F$ such that

$$|P_1| + |P'_2| = |P'_1| + |P_R| + 1 + |P'_2| \geq 2^n - 2|F| - 3.$$

Case 4: If A, B are both subcubes, say $u, x \in V(Q_L)$ and $v, y \in V(Q_R)$, then we proceed similarly as in Case 2, Subcase (ii) of Lemma 9.4. If u and x, or v and y are of opposite parity, then from Corollary 6.4 we obtain a long F_L-free ux-path P_L in Q_L and a long F_R-free vy-path P_R in Q_R such that $|P_L| + |P_R| \geq 2^n - 2|F| - 3$. Hence P_L, P_R is a long F-free AB-routing in Q_n.

Since $A \cup B$ is not monopartite, it remains to consider the case when u and x have the same parity opposite to the parity of v and y. We choose two vertices $a, b \in V(Q_L) \setminus F_L$ with the same parity opposite to the parity of u, and $a_R, b_R \notin F_R$. Note that such vertices exist since there are 2^{n-2} candidate vertices in Q_L with the parity opposite to the parity of u, the faulty vertices block at most $n-3$ of them, and $2^{n-2} - (n-3) \geq 2$ for $n \geq 5$. It follows that $A_L = \{u, x\}$, $B_L = \{a, b\}$ are disjoint and $A_L \cup B_L$ is not monopartite. Hence, by induction there is a long F_L-free $A_L B_L$-routing P'_1, P'_2 in Q_L. Moreover, since both paths P'_1, P'_2 have odd length, we have $|P'_1| + |P'_2| \geq 2^{n-1} - 2|F_L| - 2$. Assume that the $A_L B_L$-routing joins the vertex u with b, otherwise we switch the roles of a and b in what follows. By the definition of a, b, the sets $A_R = \{b_R, v\}$, $B_R = \{a_R, y\}$ are disjoint and $A_R \cup B_R$ is not monopartite. Hence, by induction there is a long F_R-free $A_R B_R$-routing P'_3, P'_4 in Q_R. By interconnecting P'_1, P'_2 and P'_3, P'_4 with edges aa_R, bb_R we obtain AB-routing P_1, P_2 in $Q_n - F$ such that $|P_1| + |P_2| = |P'_1| + |P'_2| + |P'_3| + |P'_4| + 2 \geq 2^n - 2|F| - 2$. □

Finally, we prove Corollary 6.7 that says for every set F of at most $n-2$ vertices of Q_n and $n \geq 4$, the graph $Q_n - F$ has an uv-path of length at least $2^n - 2|F| - 1$ for every two vertices $u, v \in V(Q_n) \setminus F$ such that $F \cup \{u, v\}$ is not monopartite.

Proof of Corollary 6.7. If $F = \emptyset$, then u and v have opposite parity, and the statement follows from a well-known fact that Q_n contains a Hamiltonian path between every two vertices of opposite parity. Otherwise, there exists $f \in F$ such that $\{u, v, f\}$ is not monopartite. Applying Theorem 6.6 for $A = \{u, f\}$, $B = \{v, f\}$, $F' = F \setminus \{f\}$ we obtain vertex-disjoint paths P_1, P_2 such that P_1 joins u and v, P_2 contains only f, and $|P_1| + |P_2| \geq 2^n - 2|F'| - 3$. Hence $|P_1| \geq 2^n - 2|F| - 1$, and P_1 is the desired path. $\square$

Chapter 10

Potential – overview

In this chapter we give an overview of proofs of Theorems 6.5 and Theorem 6.2 and explain the general ideas.

10.1 Preliminaries

The n-dimensional hypercube Q_n is the (bipartite) graph with all binary vectors of length n as vertices and edges joining every two vertices that differ in exactly one coordinate. Let $\mathbf{0}$ denote the vertex of Q_n consisting of all 0's. For every $i \in [n] = \{1, 2, \ldots, n\}$ let e_i denote the vertex with 1 exactly in the i-th coordinate. Furthermore, for every distinct $i, j \in [n]$ let $e_{i,j}$ denote the vertex with 1 exactly in the i-th and j-th coordinate.

Let $d(u, v)$ be the (Hamming) distance of vertices u and v in Q_n, i.e. the number of coordinates where u and v differ. Recall that the *weight* $|u|$ of a vertex u is the number of 1's in u, i.e. $|u| = d(u, \mathbf{0})$. The vertices of even and odd weight, respectively, form bipartite classes of Q_n. The *parity* of a vertex u is the parity of its weight $|u|$. Hence, two vertices have the same parity if and only if they are in the same bipartite class. The *k-th level* of Q_n is the set of vertices of weight k for $0 \le k \le n$.

Clearly, Q_n has a regular degree n. Let $N(u)$ be the set of neighbors of a vertex u in Q_n, and let $N^+(u)$ and $N^-(u)$ be the sets neighbors of u with weight $|u| + 1$ and $|u| - 1$, respectively. It is well-known that every two vertices of Q_n have 0 or 2 common neighbors.

In order to apply induction, we need to split the hypercube Q_n into two $(n-1)$-dimensional subcubes $Q_{i:L}$ and $Q_{i:R}$. This is obtained by fixing some coordinate $i \in [n]$. Formally, we define the subcube $Q_{i:L}$ as the subgraph of Q_n induced by vertices that have 0 on the i-th coordinate. Similarly, the subcube $Q_{i:R}$ is the subgraph of Q_n induced by vertices that have 1 on the i-th coordinate. For a vertex x of $Q_{i:L}$, let x_R be the (only) neighbor of x in $Q_{i:R}$. Similarly for a vertex x of $Q_{i:R}$, let x_L be the (only) neighbor of x in $Q_{i:L}$.

Assume that F is a given set of faulty vertices of Q_n. The vertices of Q_n which are not in F are called *F-free*. For every $i \in [n]$ we define $F_{i:L}$ and $F_{i:R}$ to be the sets of faulty vertices in $Q_{i:L}$ and $Q_{i:R}$, respectively. Let F^k be the set of vertices of F from level k (i.e. of weight k) for $0 \le k \le n$. Similarly, let $F^{\ge k}$ be the set of vertices of F from level at least k. Furthermore, we define $F^k_{i:L} = F^k \cap F_{i:L}$ and $F^k_{i:R} = F^k \cap F_{i:R}$. For a vertex u of Q_n let $F(u)$ be the set of faulty neighbors of u, i.e. $F(u) = F \cap N(u)$.

Let A_F be the $|F| \times n$ matrix whose rows are the binary vectors representing the vertices of F. Let $|A_F|$ be the number of ones in A_F. Clearly, $|A_F|$ is the sum of $|x|$ over all $x \in F$. Note that $|F_{i:L}|$ and $|F_{i:R}|$ are the numbers of zeros and ones, respectively, in the i-th column of A_F. By symmetry of Q_n, we assume that

$$|F_{i:L}| \geq |F_{i:R}| \text{ for every dimension } i \in [n]. \tag{10.1}$$

Indeed, by exchanging zeros and ones in those columns $i \in [n]$ where $|F_{i:L}| < |F_{i:R}|$ we obtain an automorphism of Q_n that maps the set F to a new set satisfying the condition (10.1).

To apply Theorem 6.3 we need to bound the number $\alpha(F)$ of vertices of Q_n that have at least 4 neighbors in F.

Proposition 10.1. *For every set $F \subseteq V(Q_n)$ it holds that*

$$\alpha(F) \leq \min\left\{\frac{n|F|}{4}, \frac{\binom{|F|}{2}}{3}\right\}.$$

Proof. Every vertex from F has n neighbors in Q_n, but every vertex x with $|F(x)| \geq 4$ has at least 4 neighbors in F. Hence, $\alpha(F) \leq n|F|/4$.

In order to prove the second inequality of this proposition we compute the number p of pairs of incident edges ux and vx of Q_n where $u, v \in F$ are distinct neighbors of x. Since every two vertices u and v of Q_n have at most 2 neighbors in common, we have $p \leq 2\binom{|F|}{2}$. On the other hand, every vertex x with $|F(x)| \geq 4$ has at least $\binom{4}{2} = 6$ pairs of vertices from F in its neighborhood, so $6\alpha(F) \leq p$. Hence, $\alpha(F) \leq \binom{|F|}{2}/3$. □

Proposition 10.2. *For every set $F \subseteq V(Q_n)$ with $|F| \leq 6$ it holds that $\alpha(F) \leq 2$.*

Proof. Suppose for a contradiction that there exist three vertices a, b and c in Q_n such that $|F(a)|, |F(b)|, |F(c)| \geq 4$. Without lost of generality we assume that $a = \mathbf{0}$. Hence, there are at least 4 faulty vertices in the first level. Since there remain at most two vertices in $F \setminus F(a)$, the vertices b and c both share exactly 2 faulty neighbors with the vertex a, so they are in the second level. Furthermore, it follows that the vertices b and c share two neighbors $x, y \in F^3$, so (b, x, c, y) forms a cycle of length 4. But this contradicts the structure of Q_n since every cycle of length 4 in Q_n is contained in exactly 3 consecutive levels. □

10.2 Overview of the proofs

The proofs of Theorems 6.2 and 6.5 have very similar structure. In both theorems we are given a set of faulty vertices F in Q_n, but the maximal cardinality of F differs. For general purposes, let us denote the maximal cardinality of F by $z(n)$. In Theorem 6.2 we have $z(n) = \binom{n}{2} - 2$, and in Theorem 6.5 we have $z(n) = \left\lfloor \frac{n^2+n-4}{4} \right\rfloor$.

Both proofs proceed by induction on the dimension n. Fortunately, the base of induction for $n = 5$ is already known in both cases. For Theorem 6.2 it directly follows from the following result.

Theorem 10.3 (Castañeda and Gotchev [12])**.** *For every set F of at most $3n - 7$ vertices in Q_n and $n \geq 5$, the graph $Q_n - F$ contains a cycle of length at least $2^n - 2|F|$.*

For Theorem 6.5, the base of induction for $n = 5$ follows from Theorem 6.3 since $2n - 4 = \left\lfloor \frac{n^2+n-4}{4} \right\rfloor$, and the condition that $|F(u)|, |F(v)| \leq 3$ implies that $N(u) \nsubseteq F \cup \{v\}$ and $N(v) \nsubseteq F \cup \{u\}$ for $n = 5$.

Hence, our task remains to prove the induction step for both Theorems 6.2 and 6.5. Although they are applied in the proofs of each other, note that it is done in a correct way, since the induction steps proceed together. That is, the statements of Theorem 6.2 and Theorem 6.5 for n requires only that

$$\text{the statements of Theorem 6.2 and Theorem 6.5 hold for } n-1. \tag{10.2}$$

In the first part of the induction steps we assume that

$$\text{there exists a dimension } i \in [n] \text{ such that } |F_{i:L}|, |F_{i:R}| \leq z(n-1). \tag{10.3}$$

In this case in Theorem 6.5 we proceed directly by applying induction (10.2) on both $Q_{i:L}$ and $Q_{i:R}$. In Theorem 6.2 we obtain from (10.1) that[1]

$$|F_{i:R}| \leq \left\lfloor \frac{|F|}{2} \right\rfloor \leq \left\lfloor \frac{\binom{n}{2} - 2}{2} \right\rfloor = \left\lfloor \frac{(n-1)^2 + (n-1) - 4}{4} \right\rfloor .$$

Therefore, we may directly apply induction (10.2): Theorem 6.2 in $Q_{i:L}$ and Theorem 6.5 in $Q_{i:R}$.

10.3 Potentials

In the second part of both proofs we assume that (10.3) does not hold. The assumption (10.1) implies that

$$|F_{i:L}| > z(n-1) \text{ for every dimension } i \in [n]. \tag{10.4}$$

Now we introduce up to our knowledge a new method of so called *potentials* which is used in the both proofs of Theorems 6.2 and 6.5.

Let $k(n) = z(n) - z(n-1) - 1$. Note that if (10.4) holds, then $|F_{i:R}| = |F| - |F_{i:L}| \leq k(n)$ for every dimension $i \in [n]$. We define the *potentials* of the set F as follows:

- $\phi_0(F) = 2(1 - |F^0|) = \begin{cases} 0 & \text{if } \mathbf{0} \in F \\ 2 & \text{if } \mathbf{0} \notin F, \end{cases}$
- $\phi_1(F)$ is the number of F-free vertices in the first level, i.e. $\phi_1(F) = n - |F^1|$,
- $\phi_{\geq 3}(F)$ is the sum of $|x| - 2$ over all faulty vertices x in level at least 3,
- $\phi_{dim}(F)$ is the sum of $|F_{i:L}| - z(n-1) - 1$ over all dimensions $i \in [n]$,
- $\phi(F) = \phi_0(F) + \phi_1(F) + \phi_{\geq 3}(F) + \phi_{dim}(F)$.

[1]This explains why we consider at most $\left\lfloor \frac{n^2+n-4}{4} \right\rfloor$ faulty vertices in Theorem 6.5.

Clearly, $\phi_0(F)$, $\phi_1(F)$, $\phi_{\geq 3}(F)$ are non-negative. Furthermore, it follows from (10.4) that $\phi_{dim}(F)$ is non-negative. Consequently, $\phi(F)$ is non-negative.

Intuitively, the potential $\phi_0(F) + \phi_1(F) + \phi_{\geq 3}(F)$ determines how much the set F differs from a set F' with a minimal number of ones in the matrix $A_{F'}$. If $\mathbf{0} \notin F$, we pay by $\phi_0(F) = 2$; otherwise, $\phi_0(F) = 0$. For every vertex of weight 1 which is not in F, we pay by 1 in $\phi_1(F)$. For every vertex of F which has weight at least 3, we pay its distance to the second level in $\phi_{\geq 3}(F)$. Finally, for every dimension $i \in [n]$ we know that $|F_{i:L}| > z(n-1)$ since we assume (10.4), therefore we pay in $\phi_{dim}(F)$ the number of vertices which could be moved from $F_{i:L}$ to $F_{i:R}$ so that (10.4) remains satisfied.

Observe that the definition of $\phi_{dim}(F)$ and (10.4) implies that if $\phi_{dim}(F) < n$, then there exists a dimension $i \in [n]$ such that $|F_{i:L}| = z(n-1) + 1$. Now, we compute the potential $\phi(F)$ of the set F. Note that the potential $\phi(F)$ depends only on $|F|$, $z(n)$ and $z(n-1)$.

Proposition 10.4. *If $|F| \leq z(n)$ and $|F_{i:L}| > z(n-1)$ for every dimension $i \in [n]$, then*

$$\phi(F) = nk(n) - 2z(n) + n + 2 - (n-2)(z(n) - |F|).$$

Proof. We prove the requested equality by double-counting the number of 1's in the matrix A_F. First, we sum up 1's by columns. Since

$$|F_{i:R}| = |F| - |F_{i:L}| = k(n) - (z(n) - |F|) - (|F_{i:L}| - z(n-1) - 1),$$

we have

$$|A_F| = \sum_{i \in [n]} |F_{i:R}| = nk(n) - n(z(n) - |F|) - \phi_{dim}(F).$$

Now, we sum up 1's by rows.

$$\begin{aligned} |A_F| &= \sum_{x \in F} |x| = 0\left|F^0\right| + 1\left|F^1\right| + 2\left|F^2\right| + 2\left|F^{\geq 3}\right| + \phi_{\geq 3}(F) \\ &= \phi_0(F) + \phi_1(F) + \phi_{\geq 3}(F) + 2|F| - n - 2. \end{aligned}$$

The requested equality follows. ◻

Let us explain informally how potentials are useful for us. Below in Proposition 11.2 we compute the particular value of $\phi(F)$ for paths when $z(n) = \left\lfloor \frac{n^2+n-4}{4} \right\rfloor$; and in Proposition 12.2 we compute it for cycles when $z(n) = \binom{n}{2} - 2$. We will see that $\phi(F)$ is small in both cases. This allows us to split Q_n into $Q_{i:L}$ and $Q_{i:R}$ so that $|F_{i:L}| = z(n-1) + 1$, i.e. there is one faulty vertex more in $F_{i:L}$ than is allowed for applying induction. In such situations we ignore one properly chosen vertex $x \in F_{i:L}$ and try to proceed directly. If the vertex x belongs to the obtained path (or cycle), we attempt to detour it.

However, those detours may also fail because of another vertex $y \in F_{i:R}$. Nevertheless, if this happens, the vertex y must contribute into $\phi_{\geq 3}(F)$. By combination of those methods we either find a long F-free path in Q_n or obtain a contradiction with a small potential $\phi(F)$.

Chapter 11

Long paths in hypercubes with quadratic number of faults

In this chapter we prove Theorem 6.5. In what follows assume that F is a set of at most $z(n) = \left\lfloor \frac{n^2+n-4}{4} \right\rfloor$ vertices of Q_n, $n \geq 5$, and u, v are distinct vertices of $Q_n - F$ with $|F(u)|, |F(v)| \leq 3$. Recall that Theorem 6.5 says that $Q_n - F$ contains a path between u and v of length at least $2^n - 2|F| - 2$. Such path is called a long F-free uv-path.

The proof proceeds by induction on the dimension n. For $n = 5$ the statement follows from Theorem 6.3 since $|F| \leq z(5) = 6$. Now, we prove the induction step for $n \geq 6$. We divide the proof into two main parts.

11.1 Induction-friendly split

In the first part, we consider the case when Q_n can be split into $Q_{i:L}$ and $Q_{i:R}$ by a dimension $i \in [n]$ such that $|F_{i:L}|, |F_{i:R}| \leq z(n-1)$; see (10.3). In this case, we apply induction directly.

Lemma 11.1. *Let Q_n be split into subcubes $Q_{i:L}$ and $Q_{i:R}$ so that $|F_{i:L}|, |F_{i:R}| \leq z(n-1)$. Then there exists a long F-free uv-path P in Q_n. Moreover, if $|F^1_{i:L}| \geq n-2$, then $\mathbf{0} \notin P$.*

Proof. Since the dimension i is fixed, in this proof we omit the index i to simplify the notation. We distinguish two cases regarding the position of vertices u and v in Q_L and Q_R.

Case 1: If u, v are in different subcubes, say $u \in V(Q_L)$ and $v \in V(Q_R)$, then our aim is to find a vertex x in Q_L of opposite parity to the parity of u such that $x \notin F_L$, $x_R \notin F_R \cup \{v\}$ and $|F_L(x)|, |F_R(x_R)| \leq 3$. If there is a such vertex x, then by induction (10.2), Q_L has a long F_L-free ux-path P_L of length at least $2^{n-1} - 2|F_L| - 1$, Q_R has a long F_R-free $x_R v$-path P_R of length at least $2^{n-1} - 2|F_R| - 2$. Hence, their concatenation by the edge xx_R is the requested long F-free uv-path P in Q_n since

$$|P| = |P_L| + |P_R| + 1 \geq 2^{n-1} - 2|F_L| - 1 + 2^{n-1} - 2|F_R| - 2 + 1 = 2^n - 2|F| - 2.$$

Let A be the set of 2^{n-2} vertices x in Q_L with the opposite parity to the parity of u. We count for how many vertices x from A at least one of the following conditions fails: $x \notin F_L$, $x_R \notin F_R \cup \{v\}$, and $|F_L(x)|, |F_R(x_R)| \leq 3$. First, we find an upper bound on the number of vertices from A such that $x \in F_L$ or $|F_L(x)| \geq 4$.

Every vertex of $F_L \setminus A$ has $n-1$ neighbors in A, so there are at most $\frac{n-1}{4}|F_L \setminus A|$ vertices x of A such that $|F_L(x)| \geq 4$. Furthermore, we have $|F_L \cap A|$ vertices in A such that $x \in F_L$. Thus, the number of vertices x of A such that $x \in F_L$ or $|F_L(x)| \geq 4$ is at most

$$\frac{n-1}{4}|F_L \setminus A| + |F_L \cap A| \leq \frac{n-1}{4}|F_L|$$

since $n \geq 6$.

Similarly, the number of vertices x of A such that $x_R \in F_R$ or $|F_R(x_R)| \geq 4$ is at most $\frac{n-1}{4}|F_R|$. Finally, at most one vertex x of A has $x_R = v$. Altogether, we have at most $\frac{n-1}{4}|F| + 1 \leq \frac{n-1}{4}z(n) + 1$ vertices x in A such that $x \notin F_L$, $x_R \notin F_R \cup \{v\}$, and $|F_L(x)|, |F_R(x_R)| \leq 3$, which is less than $|A| = 2^{n-2}$ for $n \geq 6$. Therefore, the desired vertex x exists.

Case 2: If u, v are in the same subcube, say $u, v \in V(Q_L)$, then by induction (10.2), there exists a long F_L-free uv-path P_L in Q_L. Our aim is to find an edge xy of P_L such that $x_R, y_R \notin F_R$ and $|F_R(x_R)|, |F_R(y_R)| \leq 3$. If there is such edge xy, then by induction, Q_R contains a long F_R-free $x_R y_R$-path P_R. By replacing the edge xy in P_L with the path (x, P_R, y), we obtain the requested long F-free uv-path P in Q_n since

$$|P| = |P_L| + |P_R| + 1 \geq 2^{n-1} - 2|F_L| - 2 + 2^{n-1} - 2|F_R| - 1 + 1 = 2^n - 2|F| - 2.$$

The path P_L has at least $2^{n-1} - 2|F_L| - 2$ edges. Every vertex z in Q_R such that $z \in F_R$ or $|F_R(z)| \geq 4$ can block at most two edges xy of P_L. We find an upper bound on the number of such vertices z.

By Proposition 10.1, there are $\alpha(F_R) \leq \min\left\{\frac{n-1}{4}|F_R|, \binom{|F_R|}{2}/3\right\}$ vertices z in Q_R such that $|F_R(z)| \geq 4$. Hence, the number of edges xy of P_L such that $x_R, y_R \notin F_R$ and $|F_R(x_R)|, |F_R(y_R)| \leq 3$ is at least

$$|P_L| - 2(|F_R| + \alpha(F_R)) \geq 2^{n-1} - 2|F| - 2\alpha(F_R) - 2 \geq \begin{cases} 2^{n-1} - 2z(n) - 2\binom{z(n-1)}{2}/3 - 2 \\ 2^{n-1} - 2z(n) - \frac{n-1}{2}z(n-1) - 2, \end{cases}$$

which is positive for $n = 6$ in the first case, and for $n \geq 7$ in the latter one. Therefore, the desired edge xy exists.

It remains to prove the second part of the statement. Assume that $|F_L^1| \geq n-2$. Since the vertex $\mathbf{0}$ has $n-1$ neighbors in Q_L, at most one of them is F_L-free. Recall that each endvertex of the path P_L has at most 3 neighbors in F_L and $n \geq 6$. Hence, the path P_L does not contain the vertex $\mathbf{0}$, and therefore also $\mathbf{0} \notin P$. □

11.2 Potentials

In the second part of the proof of Theorem 6.5 we assume that (10.3) fails, i.e. (10.4) holds.

By substituting $z(n) = \left\lfloor \frac{n^2+n-4}{4} \right\rfloor$ and $k(n) = z(n) - z(n-1) - 1$ into Proposition 10.4 we immediatelly obtain the following table of values of the potential $\phi(F)$ for $n = 4m + (n \bmod 4)$ where $m = \lfloor m/4 \rfloor$. Note that $k(n) \leq \left\lfloor \frac{n-1}{2} \right\rfloor$ in the all four cases.

n	$z(n)$	$k(n)$	$\phi(F)$
$4m$	$4m^2+m-1$	$2m-1$	$4-2m-(n-2)(z(n)-\lvert F\rvert)$
$4m+1$	$4m^2+3m-1$	$2m-1$	$4-4m-(n-2)(z(n)-\lvert F\rvert)$
$4m+2$	$4m^2+5m$	$2m$	$4-2m-(n-2)(z(n)-\lvert F\rvert)$
$4m+3$	$4m^2+7m+2$	$2m+1$	$4-(n-2)(z(n)-\lvert F\rvert)$

Lemma 11.2. *If $|F_{i:L}| > z(n-1)$ for every dimension $i \in [n]$, then $|F| = z(n)$. Moreover, $\phi(F) = 2$ for $n = 6$ and $\phi(F) \leq 4$ for $n \geq 7$.*

Proof. Since $\phi(F) \geq 0$ and $n \geq 6$, we have $(n-2)(z(n)-|F|) = 0$ in the above table, so $|F| = z(n)$. The above table also implies the second part of this statement. □

In the rest of the proof we proceed by contradiction, so let us suppose that F is a set of at most $z(n)$ vertices of Q_n and u, v are distinct vertices with $|F(u)|, |F(v)| \leq 3$ such that

$$Q_n \text{ does not contain a long } F\text{-free } uv\text{-path.} \tag{11.1}$$

Recall that Lemma 11.1 implies that the assumption (10.3) fails. In the next lemma we consider the configurations when faulty vertex $\mathbf{0}$ has at most two F-free neighbors in Q_n.

Lemma 11.3. *$\mathbf{0} \notin F$ or $|F^1| \leq n-2$.*

Proof. For a contradiction, suppose $\mathbf{0} \in F$ and $|F^1| \geq n-1$. Since $n \geq 6$ and $\phi_{dim}(F) \leq 4$ by Lemma 11.2, there exists $i \in [n]$ such that $|F_{i:L}| = z(n-1)+1$. It follows that (10.3) holds for the set $F' = F \setminus \{\mathbf{0}\}$ as $\mathbf{0} \in F_{i:L}$. Thus, there exists a long F'-free uv-path P in Q_n by Lemma 11.1. Since $|F^1_{i:L}| \geq n-2$, Lemma 11.1 implies that the path P does not contain the vertex $\mathbf{0}$. Therefore, P is also a long F-free uv-path contrary to (11.1). □

Corollary 11.4. *$\phi_{\geq 3}(F) \leq 2$ for $n \geq 7$, and $\phi_{\geq 3}(F) = 0$ for $n = 6$.*

Proof. Lemma 11.3 implies that $\phi_0(F)+\phi_1(F) \geq 2$. The rest follows from Lemma 11.2. □

The following corollary shows that we can use Theorem 6.2 to find a long $F_{i:L}$-free cycle in $Q_{i:L}$ for every dimension $i \in [n]$.

Corollary 11.5. *$|F_{i:L}| \leq \binom{n-1}{2} - 2$ for every $i \in [n]$.*

Proof. For a contradiction, suppose $|F_{i:L}| > \binom{n-1}{2} - 2$ for some $i \in [n]$. Since $|F_{i:L}| \leq |F| = z(n) = \left\lfloor \frac{n^2+n-4}{4} \right\rfloor$ and $n \geq 6$, the only possible values are $n = 6$ and $|F_{i:L}| = z(6) = 9$. Thus $|F_{i:R}| = 0$, and consequently, $\phi_{dim}(F) \geq 2$. But this contradicts $\phi(F) = 2$ from Lemma 11.2 and $\phi_0(F)+\phi_1(F) \geq 2$ from Lemma 11.3. □

Lemma 11.6. *If $\phi_{\geq 3}(F) \geq 2$ or $n = 6$, then $|F^1| = n$.*

Proof. If $\phi_{\geq 3}(F) \geq 2$ or $n = 6$, then by Lemma 11.2,

$$\phi_0(F) + \phi_1(F) + \phi_{dim}(F) \leq 2. \tag{11.2}$$

Thus, if $\mathbf{0} \notin F$, then $|F^1| = n$ by the definition of potentials $\phi_0(F)$ and $\phi_1(F)$.

Now suppose that $\mathbf{0} \in F$. Consequently, $|F^1| = n-2$ by Lemma 11.3 and (11.2). Let $i \in [n]$ be such that $e_i \notin F^1$. Since $\phi_{dim}(F) = 0$ by (11.2), we have $|F_{i:L}| = z(n-1)+1$. It follows that (10.3) holds for the set $F' = F \setminus \{\mathbf{0}\}$. Hence, there exists a long F'-free uv-path P in Q_n by Lemma 11.1. Moreover, since $|F^1_{i:L}| = n-2$, the path P does not contain the vertex $\mathbf{0}$ by the second part of Lemma 11.1. Therefore, P is also a long F-free uv-path, which is contrary to (11.1). □

In the next lemma we consider the configurations when u or v is $\mathbf{0}$ or there exists a dimension $i \in [n]$ such that $u, v \in V(Q_{i:R})$.

Lemma 11.7. *$u, v \neq \mathbf{0}$ and for every $i \in [n]$ it holds that $u_i = 0$ or $v_i = 0$.*

Proof. Without lost of generality, suppose for a contradiction that $u = \mathbf{0}$. Then $\phi_0(F) + \phi_1(F) \geq n-1$ by the definition of potentials $\phi_0(F)$ and $\phi_1(F)$ since $|F^1| = |F(u)| \leq 3$, which contradicts Lemma 11.2. Thus, the first part holds.

For the second part, suppose that $u_i = v_i = 1$ for some $i \in [n]$, so $u, v \in V(Q_{i:R})$. Since $|F_{i:L}| \leq \binom{n-1}{2} - 2$ by Corollary 11.5, there is a long $F_{i:L}$-free cycle C_L in $Q_{i:L}$ by induction (10.2). Let ab be an edge of C_L such that $a_R, b_R \notin F_{i:R}$ and $\{a_R, b_R\} \neq \{u, v\}$, and put $A = \{a_R, b_R\}$, $B = \{u, v\}$. Note that such edge ab exists since $|C_L| \geq 2^{n-1} - 2|F_{i:L}|$, every vertex of $F_{i:R} \cup \{u, v\}$ blocks at most 2 edges of C_L, and $2^{n-1} - 2|F| - 4 \geq 1$ for $n \geq 6$. Since $|F_{i:R}| \leq k(n) \leq \lfloor \frac{n-1}{2} \rfloor \leq n-3$, by Theorem 6.6 there is a long $F_{i:R}$-free AB-routing P_1, P_2 in $Q_{i:R}$. After interconnecting the path $C_L - \{ab\}$ and P_1, P_2 with the edges aa_R, bb_R we obtain an uv-path in $Q_n - F$ of length

$$|C_L| + |P_1| + |P_2| + 1 \geq 2^{n-1} - 2|F_{i:L}| + 2^{n-1} - 2|F_{i:R}| - 3 + 1 = 2^n - 2|F| - 2,$$

which contradicts with (11.1). □

Next, we describe a construction based on long $F_{i:L}$-free cycles in $Q_{i:L}$. Without loss of generality, we assume that

$$\text{if } |u| = 1 \text{ or } |v| = 1, \text{ then } |u| = 1; \tag{11.3.1}$$

$$\text{if } |u|, |v| \geq 2 \text{ and, } |u| \geq 3 \text{ or } |v| \geq 3, \text{ then } |u| \geq 3; \tag{11.3.2}$$

$$\text{if } |u| = |v| = 2, \text{ then } |F^1 \cap N(u)| \geq |F^1 \cap N(v)|; \tag{11.3.3}$$

otherwise, we switch the roles of u and v. The last condition says that the vertex u has at least the same number of faulty neighbors in the first level as the vertex v.

By Lemma 11.7, there exists a dimension $i \in [n]$ such that $u_i = 0$ and $v_i = 1$, so $u \in V(Q_{i:L})$ and $v \in V(Q_{i:R})$. Since $|F_{i:L}| \leq \binom{n-1}{2} - 2$ by Corollary 11.5, there is an $F_{i:L}$-free cycle C_L in $Q_{i:L}$ by induction (10.2). For the rest of this section, this splitting of Q_n into $Q_{i:L}$ and $Q_{i:R}$, and the cycle C_L are fixed. For ease of notation, we omit the index i in the rest of this section.

For a vertex $z \in C_L$ let $c(z), a(z), z, b(z), d(z)$ be a subpath of C_L, and let $M(z) = \{a(z), b(z), c(z), d(z)\}$. For example, see the set $M(u)$ on Figure 11.1(a). We say that a vertex x of Q_L is *blocked* if $x_R \in F_R \cup \{v\}$. Furthermore, we say that $M(z)$ is blocked if every vertex of $M(z)$ is blocked. The following proposition gives a sufficient condition which guarantees that the vertex x cannot be blocked by the vertex v.

Proposition 11.8. *For every vertex x of Q_L, if $|x| \geq d(x, u)$, then $x_R \neq v$.*

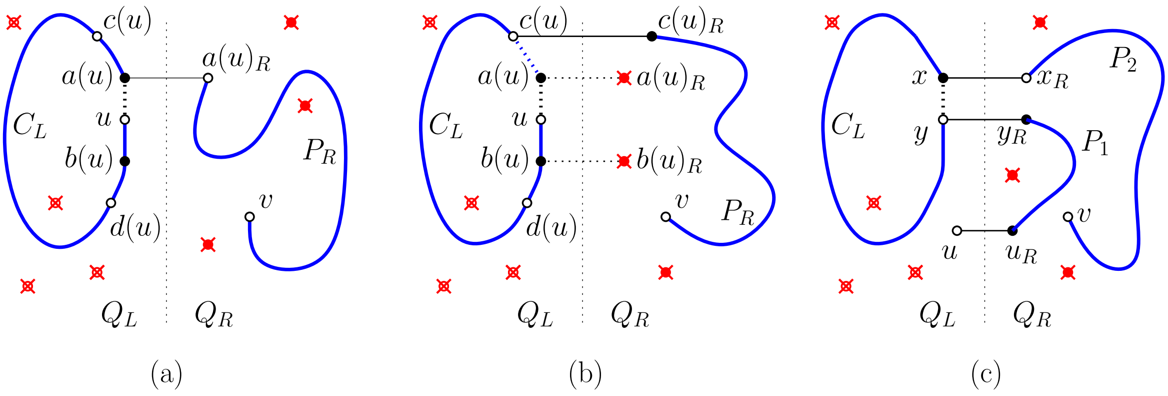


Figure 11.1: The construction in Lemma 11.9.

Proof. Recall that $i \in [n]$ is the fixed splitting dimension of Q_n into Q_L and Q_R, so $u_i = x_i = 0$ and $v_i = 1$. If $|x| \geq d(x,u)$, then there exists $j \in [n] \setminus \{i\}$ such that $u_j = x_j = 1$ since $u \neq \mathbf{0}$ by Lemma 11.7. Furthermore, $v_j = 0$ by Lemma 11.7. Hence $d(x,v) \geq 2$. $\square$

The next construction gives us many blocked vertices. For a vertex $x \in V(Q_L) \setminus F_L$ and the cycle C_L let $\mathcal{S}(x)$ denote the following statement:

$$\mathcal{S}(x) := \begin{cases} M(x) \text{ is blocked} & \text{if } x \in C_L, \\ x \text{ is blocked} & \text{if } x \notin C_L. \end{cases}$$

Lemma 11.9. *Let C_L be a long F_L-free cycle in Q_L, $u \in V(Q_L)$, and $v \in V(Q_R)$. Then $\mathcal{S}(u)$ holds. Moreover, if $u \notin C_L$, then $\mathcal{S}(z)$ holds also for every neighbor z of u in $Q_L - F_L$.*

Proof. *Case 1: $u \in C_L$.*
First, suppose that $a(u)$ or $b(u)$ is not blocked, say $a(u)_R \notin F_R \cup \{v\}$. See Figure 11.1(a) for an illustration. Then Q_R contains a long F_R-free $a(u)_R v$-path P_R by Corollary 6.4 since $|F_R| \leq k(n) \leq \left\lfloor \frac{n-1}{2} \right\rfloor$. By connecting P_R and the path $C_L - \{ua(u)\}$ with the edge $a(u)a(u)_R$ we obtain an uv-path in $Q_n - F$ of length

$$|C_L| + |P_R| \geq 2^{n-1} - 2|F_L| + 2^{n-1} - 2|F_R| - 2 = 2^n - 2|F| - 2,$$

which is a contradiction with (11.1).

Second, suppose that $c(u)$ or $d(u)$ is not blocked, say $c(u)_R \notin F_R \cup \{v\}$; see Figure 11.1(b). Since $a(u), b(u)$ are blocked, it follows that $F_R \cup \{c(u)_R, v\}$ is not monopartite. Thus, by Corollary 6.7 there is an $c(u)_R v$-path P_R in $Q_R - F_R$ of length at least $2^{n-1} - 2|F_R| - 1$. By connecting P_R and the path $C_L \setminus \{ua(u), a(u)c(u)\}$ with the edge $c(u)c(u)_R$ we obtain an uv-path in $Q_n - F$ of length

$$|C_L| + |P_R| - 1 \geq 2^{n-1} - 2|F_L| + 2^{n-1} - 2|F_R| - 2 = 2^n - 2|F| - 2,$$

which is a contradiction with (11.1).

Case 2: $u \notin C_L$. Next, suppose that the vertex u is not blocked. Then, we choose an edge xy on C_L such that $x_R, y_R \notin F_R$. Note that such edge xy exists since $|C_L| \geq 2^{n-1} - 2|F_L|$, every vertex of F_R blocks at most 2 edges of C_L, and $2^{n-1} - 2|F| \geq 1$

for $n \geq 6$. See Figure 11.1(c) for an illustration. For sets $A = \{x_R, y_R\}$, $B = \{u_R, v\}$ we have that $A \neq B$ and $A \cup B$ is not monopartite. Hence, by Theorem 6.6 there is a long F_R-free AB-routing P_1, P_2 in Q_R. By connecting u, the path $C_L - \{xy\}$, and P_1, P_2 with the edges xx_R, yy_R, uu_R, we obtain an uv-path in $Q_n - F$ of length

$$|C_L| + |P_1| + |P_2| + 2 \geq 2^{n-1} - 2|F_L| + 2^{n-1} - 2|F_R| - 1 = 2^n - 2|F| - 1,$$

which is contradiction with (11.1). Therefore, the statement $\mathcal{S}(u)$ is established.

Finally, suppose that $\mathcal{S}(z)$ does not hold for some neighbor $z \in V(Q_L) \setminus F_L$ of u. Then, by the same constructions as above, there is a long F-free zv-path P in Q_n. Note that $u \notin P$. By prolonging P with the edge uz we obtain a long F-free uv-path in Q_n, contrary to (11.1). □

In the next two lemmas we consider the configurations when the weight of the vertex u or v is not 2.

Lemma 11.10. $|u|, |v| \geq 2$.

Proof. Recall that $|u|, |v| \geq 1$ by Lemma 11.7. Suppose that $|u| = 1$ or $|v| = 1$, so $|u| = 1$ by the assumption (11.3.1). It follows that $|F^1| \leq n - 1$, so $n \geq 7$ by Lemma 11.6. First, we assume that $u \in C_L$. Then $M(u)$ is blocked by Lemma 11.9. Clearly, at least one of $a(u)$ and $b(u)$ has weight 2, say $a(u)$, and $b(u)$ has weight 0 or 2. If $|b(u)| = 2$, then $a(u)_R, b(u)_R \in F_R$ by Proposition 11.8 and consequently, $\phi_{\geq 3}(F) \geq 2$ contrary to Lemma 11.6. Otherwise $|b(u)| = 0$ and consequently, $\mathbf{0} \notin F$, $|F^1| \leq n - 2$, and $\phi_{\geq 3}(F) \geq 1$ since $a(u)_R \in F_R$ by Proposition 11.8. Hence $\phi_0(F) + \phi_1(F) + \phi_{\geq 3}(F) \geq 5$, which contradicts Lemma 11.2.

Now, we have $u \notin C_L$. If u has a neighbor z on C_L with $|z| = 2$, then $M(z)$ is blocked by Lemma 11.9. Note that $a(z)$ or $b(z)$ belong to the third level, say $|a(z)| = 3$, since z has exactly two neighbors in the first level and one of them is $u \notin C_L$. Hence, we have $a(z)_R \in F_R$ by Proposition 11.8 and consequently, $\phi_{\geq 3}(F) \geq 2$, which contradicts Lemma 11.6.

Otherwise, no neighbor z of u in $Q_L - F_L$ with $|z| = 2$ belongs to C_L. Since $|F(u)| \leq 3$, the vertex u has at least $n - 5$ neighbors z in $Q_L - F_L$ with $|z| = 2$. By Lemma 11.9, they are all blocked, but by Proposition 11.8, they are not blocked by the vertex v. Hence, $\phi_{\geq 3}(F) \geq n - 5 \geq 2$ which contradicts Lemma 11.6. □

Lemma 11.11. $|u|, |v| \leq 2$.

Proof. Suppose that $|u| \geq 3$ or $|v| \geq 3$, so $|u| \geq 3$ by the assumption (11.3.2). First, we consider the case when $u \in C_L$. Then $M(u)$ is blocked by Lemma 11.9. Since $a(u)$ and $b(u)$ belong to level at least 2, we have $a(u)_R, b(u)_R \in F_R$ by Proposition 11.8, so we obtain that $\phi_{\geq 3}(F) \geq 2$. Thus, $|F^1| = n$ by Lemma 11.6. Hence, the vertices $c(u)$ and $d(u)$ have weight at least 2, and they are not blocked by the vertex v by Proposition 11.8. Consequently $\phi_{\geq 3}(F) \geq 4$, which contradicts Corollary 11.4.

Now, we have $u \notin C_L$, so the vertex u is blocked by Lemma 11.9. Since $u_R \in F_R$ by Proposition 11.8, we have $\phi_{\geq 3}(F) \geq 2$ and consequently, $|F^1| = n$ by Lemma 11.6. Furthermore, for an arbitrary neighbor $z \in V(Q_L) \setminus F_L$ of u we obtain from Lemma 11.9 that z is blocked if $z \notin C_L$, or $a(z)$ is blocked if $z \in C_L$. In both cases have another blocked vertex at distance at most 2 from u and in level at least 2, so $\phi_{\geq 3}(F) \geq 3$ by Proposition 11.8, which contradicts Corollary 11.4. □

By the previous two lemmas we have $|u| = |v| = 2$. Let u_1, u_2 and v_1, v_2 be the neighbors of u and v of weight 1, respectively. Note that from Lemma 11.7 it follows that these four vertices are distinct.

Lemma 11.12. *$u_1 \in F$ or $u_2 \in F$.*

Proof. Suppose that $u_1, u_2 \notin F$. From the assumption (11.3.3) it follows that also $v_1, v_2 \notin F$. Thus, $\phi_1(F) \geq 4$. If $u \in C_L$, then $M(u)$ is blocked by Lemma 11.9, and $c(u)$ or $d(u)$ is in level at least 2, say $|c(u)| \geq 2$, since they have the same parity as u. By Proposition 11.8 we have $c(u)_R \in F_R$ and consequently, $\phi_{\geq 3}(F) \geq 1$. Hence, we obtain that $\phi_1(F) + \phi_{\geq 3}(F) \geq 5$, a contradiction with Lemma 11.2.

If $u \notin C_L$, the vertex u is blocked by Lemma 11.9. By Proposition 11.8 we have $u_R \in F_R$ and consequently, $\phi_{\geq 3}(F) \geq 1$. Similarly as above, we obtain that $\phi_1(F) + \phi_{\geq 3}(F) \geq 5$, a contradiction with Lemma 11.2. □

The end of the proof of Theorem 6.5. If $u \in C_L$, then $M(u)$ is blocked by Lemma 11.9. From Lemma 11.12 it follows that $a(u)$ or $b(u)$ is in the third level, say $|a(u)| = 3$. Furthermore, $|c(u)| \geq 2$. Since $a(u)_R, c(u)_R \in F_R$ by Proposition 11.8, we have $\phi_{\geq 3}(F) \geq 3$, which contradicts Corollary 11.4.

Finally, if $u \notin C_L$, then u is blocked by Lemma 11.9. Let $z \in V(Q_L) \setminus F_L$ be an arbitrary neighbor of u with $|z| = 3$. Then by Lemma 11.9, z is blocked, or the vertices $a(z)$ and $b(z)$ of weight at least 2 are blocked. By Proposition 11.8, $u_R, z_R \in F_R$ in the first case, and $u_R, a(z)_R, b(z)_R \in F_R$ in the latter case. Altogether, we obtain that $\phi_{\geq 3}(F) \geq 3$, which is a final contradiction with Corollary 11.4.

Therefore, we conclude that the contradicted assumption (11.1) is false, i.e. the statement of Theorem 6.5 holds. □

Chapter 12

Long cycles in hypercubes with optimal number of faults

In this chapter we prove the main Theorem 6.2 which says that for every set of faulty vertices F of Q_n of size at most $\binom{n}{2} - 2$ there exists a cycle in $Q_n - F$ of length at least $2^n - 2|F|$, where $n \geq 4$. Such cycle is called a long F-free cycle.

Fu [45] proved that there exists a long F-free cycle if $|F| \leq 2n - 4$, where $n \geq 3$, which implies that Theorem 6.2 holds for $n = 4$. Theorem 10.3 implies the base of induction of Theorem 6.2 for $n = 5$.

In the induction step of the proof of Theorem 6.2 for n, we assume that both Theorems 6.2 and 6.5 hold for $n - 1$; see (10.2). Let us consider a fixed set F of at most $\binom{n}{2} - 2$ faulty vertices in Q_n, where $n \geq 6$. Furthermore, we assume that $|F_{i:L}| \geq |F_{i:R}|$ for every dimension $i \in [n]$; see (10.1).

12.1 Induction-friendly split

In the first part of the proof of Theorem 6.2 we assume that there exists a dimension $i \in [n]$ such that $|F_{i:L}|, |F_{i:R}| \leq \binom{n-1}{2} - 2$; see (10.3). In this case we apply induction (10.2) in both $Q_{i:L}$ and $Q_{i:R}$ to construct a long F-free cycle Q_n. Moreover, the following lemma also considers other conditions in which we can simply find a long F-free cycle in the same way. Those conditions are useful later.

Lemma 12.1. *If there exists a dimension $i \in [n]$ such that at least one of the following conditions holds, then there exists a long F-free cycle in Q_n.*

1. *There exists a long $F_{i:L}$-free cycle C_L in $Q_{i:L}$;*
2. $|F_{i:L}| \leq \binom{n-1}{2} - 2$;
3. $|F_{i:L}| = \binom{n-1}{2} - 1$ *and there exists $x \in F_{i:L}$ having at most one $F_{i:L}$-free neighbor in $Q_{i:L}$.*

Proof. Our first aim is to find a long $F_{i:L}$-free cycle C_L in $Q_{i:L}$. If the condition (1) is satisfied, then the cycle is given. If the condition (2) is satisfied, then the cycle exists by induction (10.2).

Let us assume that the condition (3) is satisfied. Let $F' = F_{i:L} \setminus \{x\}$. By induction (10.2), there exists a long F'-free cycle C_L in $Q_{i:L}$. Since no cycle of $Q_{i:L} - F'$ contains x, the cycle C_L is also $F_{i:L}$-free.

Our next aim is to find an edge xy of C_L such that

$$x_R, y_R \notin F_{i:R} \text{ and } |F_{i:R}(x_R)|, |F_{i:R}(y_R)| \leq 3. \tag{12.1}$$

If there exists an edge xy satisfying (12.1), then by induction (10.2), there is a long $F_{i:R}$-free $x_R y_R$-path P_R in $Q_{i:R}$ since $|F_{i:R}| \leq \left\lfloor \frac{|F|}{2} \right\rfloor \leq \left\lfloor \frac{(n-1)^2+(n-1)-4}{4} \right\rfloor$. We replace the edge xy in C_L by a path (x, x_R, P_R, y_R, y) and we obtain an F-free cycle in Q_n of length at least

$$(2^{n-1} - 2|F_{i:L}| - 1) + 2 + (2^{n-1} - 2|F_{i:R}| - 1) = 2^n - 2|F|.$$

It remains to show that there exists an edge xy satisfying (12.1). Recall that $\alpha(F_{i:R})$ is the number of vertices z in $Q_{i:R}$ with $|F_{i:R}(z)| \geq 4$. There are at most $|F_{i:R}| + \alpha(F_{i:R})$ vertices that cannot be used as end-vertices of a long $F_{i:R}$-free path in $Q_{i:R}$. Since the length of C_L is at least $2^{n-1} - 2|F_{i:L}|$, the number of edges xy satisfying (12.1) is at least

$$2^{n-1} - 2|F_{i:L}| - 2\left(|F_{i:R}| + \alpha(F_{i:R})\right) \geq 2^{n-1} - 2|F| - 2\alpha(F_{i:R}) \geq 1.$$

The last inequality follows from $|F_{i:R}| \leq |F|/2$ and from

- Proposition 10.2 for $n = 6$;
- the inequality $\alpha(F_{i:R}) \leq \binom{|F_{i:R}|}{2}/3$ by Proposition 10.1 for $n = 7$;
- the inequality $\alpha(F_{i:R}) \leq \frac{(n-1)|F_{i:R}|}{4}$ by Proposition 10.1 for $n \geq 8$.

□

12.2 Potentials

In the second part of the proof of Theorem 6.2 we assume that (10.3) fails, i.e. (10.4) holds.

Let us recall that we use the following potentials, where now we have $z(n) = \binom{n}{2} - 2$.

$$\phi(F) = \phi_0(F) + \phi_1(F) + \phi_{\geq 3}(F) + \phi_{dim}(F),$$
$$\phi_0(F) = 2 - 2|F^0|, \qquad \phi_1(F) = n - |F^1|,$$
$$\phi_{\geq 3}(F) = \sum_{x \in F^{\geq 3}} (|x| - 2), \qquad \phi_{dim}(F) = \sum_{i \in [n]} (|F_{i:L}| - z(n-1) - 1).$$

By substituting $z(n) = \binom{n}{2} - 2$ and $k(n) = z(n) - z(n-1) - 1 = n - 2$ into Proposition 10.4, the next lemma follows immediately.

Lemma 12.2. *Let F be a set of faulty vertices of Q_n of size at most $\binom{n}{2} - 2$. If $|F_{i:L}| \geq \binom{n-1}{2} - 1$ for every dimension $i \in [n]$, then $|F| \geq \binom{n}{2} - 3$ and*

$$\phi(F) = \begin{cases} 6 & \text{if } |F| = \binom{n}{2} - 2 \\ 8 - n & \text{if } |F| = \binom{n}{2} - 3. \end{cases}$$

In the rest of this section we proceed by contradiction. Therefore, we consider a set of vertices F of Q_n of size at most $\binom{n}{2} - 2$ such that

$$\text{there is no long } F\text{-free cycle in } Q_n. \tag{12.2}$$

From the assumption (2) of Lemma 12.1 it follows that $|F_{i:L}| \geq \binom{n-1}{2} - 1$ and $|F_{i:R}| \leq n-2$ for every dimension $i \in [n]$; see (10.4).

It follows from Lemma 12.2 that there cannot be too many vertices in $F^{\geq 3}$ and they cannot be too far from $\mathbf{0}$. Now, we present a construction which gets a faulty vertex a and gives us another faulty vertex b_R in the level $|a|$ or $|a|+2$.

Lemma 12.3. *Let $i \in [n]$ be a dimension and let a be a given vertex of $F^k_{i:L}$. Let one of the two following conditions hold.*

1. $|F_{i:L}| = \binom{n-1}{2} - 1$,
2. $|F_{i:L}| = \binom{n-1}{2}$, $|F^1_{i:L} \setminus \{a\}| \geq n-2$, $\mathbf{0} \in F$ *and* $a \neq \mathbf{0}$.

Then, there exists $b \in V(Q_{i:L}) \cap N(a)$ such that $b_R \in F_{i:R}$. Hence, $|b_R| \in \{k, k+2\}$.

Moreover, if at least one of the three following conditions holds, then $|b_R| = k+2$.

3. *Every vertex $x \in N^-(a)$ is faulty,*
4. *for every $x \in N^-(a)$ the vertex x_R is $F_{i:R}$-free,*
5. $|F^1_{i:L}| = n-1$ *and* $k = 1$.

Proof. Let

$$F' = \begin{cases} F_{i:L} \setminus \{a\} & \text{if (1) holds,} \\ F_{i:L} \setminus \{a, \mathbf{0}\} & \text{if (2) holds.} \end{cases}$$

By induction (10.2), there exists a long F'-free cycle C_L in $Q_{i:L}$. If (2) holds, then $\mathbf{0} \notin C_L$ because $\mathbf{0}$ has at most one F'-free neighbor in $Q_{i:L}$. Since there is no long $F_{i:L}$-free cycle in $Q_{i:L}$ by the assumption (1) of Lemma 12.1 and by the contradicted assumption (12.2), the vertex a is contained in C_L.

Let b and c be two neighbors of a on C_L. If $b_R, c_R \notin F_{i:R}$, then by Theorem 6.3 there exists a long $F_{i:R}$-free b_Rc_R-path P_R in $Q_{i:R}$ since $|F_{i:R}| \leq n-2$ and b_R, c_R are not adjacent. Hence, the length of an F-free cycle obtained from C_L by removing edges ba, ac and inserting a path (b, b_R, P_R, c_R, c) is at least

$$(2^{n-1} - 2|F'|) - 2 + 2 + (2^{n-1} - 2|F_{i:R}| - 2) \geq 2^n - 2|F|.$$

Therefore, at least one of b_R and c_R belongs into $F_{i:R}$, say $b_R \in F_{i:R}$, which implies the first part of the statement.

Now, we prove the second part. Note that

$$|b_R| = \begin{cases} k & \text{if } b \in N^-(a), \\ k+2 & \text{if } b \in N^+(a). \end{cases}$$

If $b \in N^-(a)$, then neither the condition (3) nor (4) is satisfied since $b \notin F_{i:L}$ and $b_R \in F_{i:R}$. If (5) holds, then $b \in N^+(a)$; otherwise, the vertex a is the only F'-free neighbor of $b = \mathbf{0}$ in $Q_{i:L}$, and there is no cycle in $Q_{i:L} - F'$ containing $\mathbf{0}$, but $b \in C_L$. $\square$

This lemma is useful to find a faulty vertex in $F^{\geq 3}$ which increases the potential $\phi_{\geq 3}(F)$. We often combine this lemma with other observations to show that the potential $\phi(F)$ is greater than the value given by Lemma 12.2 which provides us with a contradiction. One such example follows, compare it with Lemma 11.3 in the previous section.

For practical purposes, we say that we use Lemma 12.3 with the assumption (1) on a vertex $x \in F_{i:L}$ to obtain a vertex $y \in V(Q_{i:L})$. This only means that Q_n is split by the dimension i, and we apply Lemma 12.3 for the given vertex $a = x$ such that the assumption (1) is satisfied. Then, y is the vertex b obtained by Lemma 12.3. Similarly, we say that we use Lemma 12.3 with the assumption (2) and (3) on a vertex $x \in F_{i:L}$ to obtain a vertex $z \in F_{i:R}$. This only means that the dimension i and the vertex $a = x$ satisfy both conditions (2) and (3) and z is the vertex $b_R \in F_{i:R}$ in level $|a| + 2$ obtained by Lemma 12.3. Note that $d(x, z) = 2$.

Lemma 12.4. $\mathbf{0} \notin F$ *or* $|F^1| \leq n - 2$.

Proof. For a contradiction, let us suppose that $\mathbf{0} \in F$ and $|F^1| \geq n - 1$.

If there exists a dimension i such that $|F_{i:L}| = \binom{n-1}{2} - 1$, then by Lemma 12.1 with the assumption (3) for $x = \mathbf{0} \in F$, which has at most one $F_{i:L}$-free neighbor in $Q_{i:L}$, we obtain a long F-free cycle in Q_n which is a contradiction with (12.2).

Now, we assume that there is no dimension $i \in [n]$ such that $|F_{i:L}| = \binom{n-1}{2} - 1$, so $\phi_{dim}(F) \geq n$. This is possible, by Lemma 12.2, only if $\phi_{dim}(F) = n = 6 = \phi(F)$ and hence by the definition of $\phi(F)$ we have that $|F^1| = 6$, $\mathbf{0} \in F$ and $F^{\geq 3} = \emptyset$. Note that in this case $|F_{i:L}| = \binom{n-1}{2}$ for every dimension $i \in [n]$, so we use Lemma 12.3 with the assumptions (2) and (3) on some vertex $a \in F^1_{i:L}$ to obtain a vertex in $F^3_{i:R}$, which is a contradiction with $F^{\geq 3} = \emptyset$. ∎

Lemma 12.4 implies that $\phi_0(F) + \phi_1(F) \geq 2$. Hence, $\phi_{\geq 3}(F) + \phi_{dim}(F) \leq 4$ by Lemma 12.2 which implies that

$$\text{there exists a dimension } i \in [n] \text{ such that } |F_{i:L}| = \binom{n-1}{2} - 1, \tag{12.3}$$

since $n \geq 6$. Moreover, the definition of $\phi_{dim}(F)$ implies for a given vertex x of Q_n that

$$\text{if } \phi_{dim}(F) + |x| < n, \text{ then } \exists i \in [n] \text{ such that } |F_{i:L}| = \binom{n-1}{2} - 1 \text{ and } x \in V(Q_{i:L}), \tag{12.4}$$

because at least $n - \phi_{dim}(F)$ dimensions $i \in [n]$ satisfy $|F_{i:L}| = \binom{n-1}{2} - 1$, and at most $|x|$ of those dimensions volatile $x \in V(Q_{i:L})$.

Our proof still proceeds by contradiction (12.2). In the following two lemmas we prove that $\phi_0(F) + \phi_1(F) \geq 3$. In the first one we consider the case when $\mathbf{0} \notin F$ and $|F^1| = n$; and in the second one, the case when $\mathbf{0} \in F$ and $|F^1| = n - 2$.

Lemma 12.5. $|F^1| \leq n - 1$.

Proof. For a contradiction we suppose that $|F^1| = n$. Hence, $\mathbf{0} \notin F$ by Lemma 12.4. We proceeds in three steps. First, we prove that $|F^3| \geq 1$. Next, we prove that $|F^4| \geq 1$, which we finally improve to $|F^4| \geq 2$. This is a contradiction to Lemma 12.2.

By (12.3) we split Q_n by such dimension $i \in [n]$ that $|F_{i:L}| = \binom{n-1}{2} - 1$. We use Lemma 12.3 with the assumptions (1) and (5) on some vertex of $F^1_{i:L}$ to obtain

$|F^3_{i:R}| \geq 1$. By Lemma 12.2 we know that $|F| = \binom{n}{2} - 2$ since $\phi_0(F) + \phi_{\geq 3}(F) \geq 3$ and $n \geq 6$.

We observe that $F^2_{i:L} \neq \emptyset$; otherwise $\left|F^{\geq 3}_{i:L}\right| = |F_{i:L}| - |F^1_{i:L}| = \binom{n-1}{2} - 1 - (n-1) \geq 4$ which implies $\phi_{\geq 3}(F) \geq \left|F^{\geq 3}_{i:L}\right| + |F^3_{i:R}| \geq 5$, contrary to Lemma 12.2. Hence, we use Lemma 12.3 with the assumptions (1) and (3) on some vertex of $F^2_{i:L}$ to obtain a vertex $x \in F^4_{i:R}$.

Now, we know that F^3, $F^4 \neq \emptyset$ and $0 \notin F$ which implies $\phi_{dim}(F) \leq 1$ by Lemma 12.2. Therefore, there exists a dimension j such that $|F_{j:L}| = \binom{n-1}{2} - 1$ and $x \in F^4_{j:L}$ by (12.4). We use Lemma 12.3 with the assumption (1) on the vertex x to obtain a vertex in $F^{\geq 4}_{j:R}$. Hence, $\left|F^{\geq 4}\right| \geq 2$ and $|F^3| \geq 1$, so $\phi_{\geq 3}(F) \geq 5$. It implies $\phi(F) \geq \phi_0(F) + \phi_{\geq 3}(F) \geq 7$, which is a contradiction with Lemma 12.2. $\square$

Lemma 12.6. *If* $\mathbf{0} \in F$*, then* $|F^1| \leq n - 3$.

Proof. For a contradiction we suppose that $\mathbf{0} \in F$ and $|F^1| = n - 2$. First, we prove that $\phi_{dim}(F) \geq 2$. Next, we prove that there exist two vertices x and y in $F^3_{d:R}$ for some $d \in [n]$. Finally, we show that there exist 4 distinct dimensions $d_1, d_2, d_3, d_4 \in [n]$, satisfying $x \in F^3_{d_l:R}$ for $l \in [4]$ which implies that $|x| \geq 4$, contrary to $x \in F^3$.

Let e_i and e_j be the (only) two F-free vertices in the first level. We observe that $|F_{i:L}|, |F_{j:L}| \geq \binom{n-1}{2}$; otherwise we use Lemma 12.1 with the assumption (3) on the vertex $\mathbf{0}$ to obtain a contradiction with (12.2). Therefore, $\phi_1(F) + \phi_{dim}(F) \geq 4$; and consequently, $\phi_{\geq 3}(F) \leq 2$ by Lemma 12.2.

We split Q_n by a dimension $d \in [n]$ so that $|F_{d:L}| = \binom{n-1}{2} - 1$ by (12.3). Let a^1, a^2, a^3 be arbitrary distinct vertices of $F^1_{d:L}$. Note that such vertices exist since $|F^1_{d:L}| = n - 3$ and $n \geq 6$. We use Lemma 12.3 with the assumptions (1) and (3) for every vertex a^m to obtain $b^m \in V(Q_{d:L})$ such that $b^m_R \in F^3_{d:R}$, where $m \in [3]$. Note that $|\{b^1_R, b^2_R, b^3_R\}| \leq 2$ since $\phi_{\geq 3}(F) \leq 2$. On the other hand, if $b^1_R = b^2_R = b^3_R$, then $b^1 = b^2 = b^3$; so $b^1 \in N^+(a^1) \cap N^+(a^2) \cap N^+(a^3)$, but $|N^-(b^1)| = 2$. Hence, b^1_R, b^2_R and b^3_R are two different vertices; say x_d and y_d. Furthermore, $|F^3| = \phi_{\geq 3}(F) = \phi_{dim}(F) = 2$.

Since $\phi_{dim}(F) = 2$ and $n \geq 6$, there are at least 4 distinct dimensions $d_l \in [n]$, $l \in [4]$, such that $|F_{d_l:L}| = \binom{n-1}{2} - 1$. For every dimension d_l we obtain vertices $x_{d_l}, y_{d_l} \in F^3_{d_l:R}$ in the same way as described in the previous paragraph. Since $|F^3| = 2$, the pairs of vertices x_{d_l} and y_{d_l} are the same for all $l \in [4]$; say $x_{d_1} = x_{d_2} = x_{d_3} = x_{d_4}$. But $x_{d_1} \in F^3_{d_l:R}$ for all $l \in [4]$ implies $|x_{d_1}| \geq 4$ which contradicts $x_{d_1} \in F^3$. $\square$

Note that from Lemmas 12.5 and 12.6 it follows that $\phi_1(F) + \phi_0(F) \geq 3$. Therefore, Lemma 12.2 implies the following statement since $n \geq 6$.

Corollary 12.7. $\phi_{\geq 3}(F) + \phi_{dim}(F) \leq 3$ *and* $|F| = \binom{n}{2} - 2$.

Consequently, from (12.4) we obtain that for every vertex $a \in F$

$$\text{there exists a dimension } i \in [n] \text{ such that } a \in F_{i:L} \text{ and } |F_{i:L}| = \binom{n-1}{2} - 1. \quad (12.5)$$

Let $u \vee v$ denote the vertex $w = (w_1, w_2, \ldots, w_n)$ with $w_i = u_i \vee v_i$ for all $i \in [n]$, where $\vee$ is the logical disjunction. Note that $w \in Q_{i:L}$ if and only if $u, v \in Q_{i:L}$ for every dimension $i \in [n]$.

Lemma 12.8. $F^{\geq 3} = \emptyset$.

Proof. For a contradiction, let us suppose that there exists a vertex $a \in F^{\geq 3}$. We proceed in 4 steps. First, we prove that $F^{\geq 4} = \emptyset$. Each of next three steps splits Q_n and uses Lemma 12.3 to obtain a new vertex in F^3, which implies that $|F^3| \geq 4$, contrary to Corollary 12.7. Note that those three splits use different dimensions.

If $|a| \geq 4$, then we split Q_n so that $a \in F_{i:L}$ and $|F_{i:L}| = \binom{n-1}{2} - 1$ by (12.5). Then we use Lemma 12.3 with the assumption (1) on the vertex a to obtain another faulty vertex in level at least 4, which is a contradiction with Corollary 12.7. Therefore, we assume that $F^{\geq 4} = \emptyset$ and $a \in F^3$.

We split Q_n so that $a \in V(Q_{i:L})$ and $|F_{i:L}| = \binom{n-1}{2} - 1$ by (12.5). By Lemma 12.3 with the assumption (1), there exists $b \in F_{i:R}$ such that $|b| = 3$ and $d(a, b) = 2$. Hence, $\phi_{\geq 3}(F) \geq 2$.

Let $x = a \vee b$. Since $d(a, b) = 2$ and $|a| = |b| = 3$, we have $|x| = 4$. Since $\phi_{dim}(F) \leq 1$ by Corollary 12.7, there exists a dimension j such that $x \in V(Q_{j:L})$ and $|F_{j:L}| = \binom{n-1}{2} - 1$ by (12.4). Hence $a, b \in F_{j:L}$. We use Lemma 12.3 with the assumption (1) twice on both a and b to obtain $c, d \in F^3_{j:R}$ such $d(a, c) = d(b, d) = 2$. Since $\phi_{\geq 3}(F) \leq 3$ by Corollary 12.7, we have $c = d$. Hence, $|a| = |b| = |c| = 3$ and $d(a, b) = d(a, c) = d(b, c) = 2$.

Let $y = a \vee b \vee c$. Similarly, we have $|y| \leq 5$ and $\phi_{dim}(F) = 0$, so there exists a dimension d such that $y \in V(Q_{d:L})$ and $|F_{d:L}| = \binom{n-1}{2} - 1$ by (12.4). Using Lemma 12.3 with the assumption (1) on the vertex a we obtain a faulty vertex in $F^3_{d:R}$; so $|F^3| \geq 4$, which is a contradiction with Corollary 12.7. □

Lemma 12.9. $\mathbf{0} \notin F$.

Proof. For a contradiction we suppose that $\mathbf{0} \in F$. Hence, $|F^1| \leq n-3$ by Lemma 12.6.

We observe that $F^1 = \emptyset$, otherwise we choose $x \in F^1$, we split Q_n so that $x \in F_{i:L}$ and $|F_{i:L}| = \binom{n-1}{2} - 1$ by (12.5), and by Lemma 12.3 with the assumptions (1) and (3) we obtain $F^{\geq 3} \neq \emptyset$, contrary to Lemma 12.8. Hence, $\phi_1(F) = n$ which is possible only if $n = 6$, $|F^1| = 0$, $|F^2| = 12$ and $\phi_{dim}(F) = 0$.

Since $\phi_{dim}(F) = 0$, we have $|F_{i:R}| = k(n) = n - 2 = 4$ for every dimension $i \in [n]$. Since $|F^1|, |F^{\geq 3}| = \emptyset$, only one vertex of $N^+(e_i)$ is F-free for every vertex e_i of the first level in Q_n. Therefore, for every dimension j there exists exactly one other dimension k such that $e_{j,k} \notin F$, so all dimensions are split into three pairs $\{j_1, k_1\}$, $\{j_2, k_2\}$ and $\{j_3, k_3\}$ such that $e_{j_1,k_1}, e_{j_2,k_2}, e_{j_3,k_3} \notin F$. This is satisfied up to isomorphism only by one set of faulty vertices F: the set of all vertices of level 0 or 2 except the vertices $e_{1,2}$, $e_{3,4}$ and $e_{5,6}$. By Lemma 12.1 with the assumption (1), it suffices to find a long $F_{6:L}$-free cycle in $Q_{6:L}$ which is presented on Figure 12.1. Thus, we obtain a contradiction with (12.2). □

Finally, we prove the last simple lemma which leads to a contradiction with (12.2).

Lemma 12.10. *For every dimension $i \in [n]$, if $e_i \notin F$, then $|F_{i:L}| \geq \binom{n-1}{2}$.*

Proof. Let us consider a vertex $e_i \notin F$ such that $|F_{i:L}| = \binom{n-1}{2} - 1$. There exists a vertex $x \in F^1_{i:L}$, because $\phi_1(F) \leq 4 \leq n - 2$ by Lemmas 12.2 and 12.9. We use Lemma 12.3 with the assumptions (1) and (4) on the vertex x to obtain $|F^3| \geq 1$, which is a contradiction to Lemma 12.8. □

The end of the proof of Theorem 6.2. Let us recall that $\phi_0(F) = 2$ by Lemma 12.9, which implies that $\phi_{dim}(F) + \phi_1(F) \leq 4$ by Lemma 12.2. Lemma 12.10 says that $\phi_{dim}(F) \geq \phi_1(F)$ which implies that $|F^1| \geq n - 2$. On the other hand, we know that

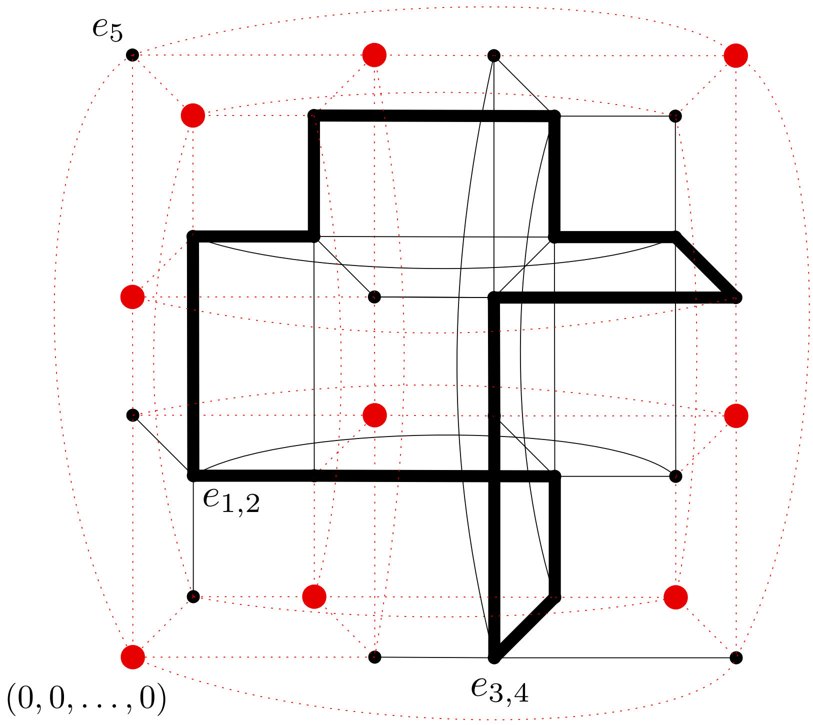


Figure 12.1: Bold points are faulty vertices and bold lines form a long $F_{6:L}$-free cycle in $Q_{6:L}$ for Lemma 12.9.

$|F^1| \leq n-1$ by Lemma 12.5. Moreover, $|F| = \binom{n}{2} - 2$ and every faulty vertex is in the level 1 or 2 by Lemmas 12.8 and 12.9.

If there exists a vertex $a \in F^2$ such that both vertices in $N^-(a)$ are faulty, then we split Q_n so that $a \in F_{i:L}$ and $|F_{i:L}| = \binom{n-1}{2} - 1$ by (12.5). Then, we use Lemma 12.3 with the assumptions (1) and (3) to obtain $|F^4| \geq 1$, which is a contradiction to Lemma 12.8. Hence, every vertex of F^2 is above some F-free vertex of level 1.

Lemma 12.10 also implies that there are at most $n-3$ faulty vertices above every F-free vertex in level 1. Since there are at most two F-free vertices in level 1, we have $|F^2| \leq 2(n-3)$. This leads to the final contradiction $3n-7 \geq |F^1|+|F^2| = |F| = \binom{n}{2}-2$ since $n \geq 6$, which finishes the proof of the main Theorem 6.2. □

Bibliography

[1] A. Alan Middleton. Numerical investigation of the thermodynamic limit for ground states in models with quenched disorder. *Physical review letters*, 83(8):1672–1675, 1999.

[2] D.J. Amalraj, N. Sundararajan, and G. Dhar. Data structure based on Gray code encoding for graphics and image processing. In *Proceedings of SPIE*, volume 1349, page 65, 1990.

[3] L.P. Arguin, M. Damron, C. Newman, and D. Stein. Uniqueness of Ground States for Short-Range Spin Glasses in the Half-Plane. *Arxiv preprint arXiv:0911.4201*, 2009.

[4] N. Ascheuer. *Hamiltonian path problems in the on-line optimization of flexible manufacturing systems*. PhD thesis, Technical University Berlin, 1995.

[5] J. Azarija, P. Gregor, and R. Škrekovski. Gray codes through edgse of perfect matchings. In preparation.

[6] J. C. Bermond, editor. *Interconnecting networks*. A special issue 37/38 of Discrete Applied Mathematics, 1992.

[7] L.N. Bhuyan and D.P. Agrawal. Generalized hypercube and hyperbus structures for a computer network. *IEEE Transactions on Computers*, 100(33):323–333, 1984.

[8] K. Binder and A.P. Young. Spin glasses: Experimental facts, theoretical concepts, and open questions. *Reviews of Modern physics*, 58(4):801–976, 1986.

[9] A.J. Bray and M.A. Moore. Chaotic nature of the spin-glass phase. *Physical review letters*, 58(1):57–60, 1987.

[10] L. M. Brègman. Certain properties of nonnegative matrices and their permanents. *Soviet Math. Dok.*, 14:945–949, 1973.

[11] J. Bruck, R. Cypher, and D. Soroker. Tolerating faults in hypercubes using subcube partitioning. *IEEE Transactions on Computers*, 41(5):599–605, 1992.

[12] N. Castañeda and I.S. Gotchev. Embedded paths and cycles in faulty hypercubes. *Journal of Combinatorial Optimization*, 2009. DOI: 10.1007.s10878-008-9205-6.

[13] M.Y. Chan and S.-J. Lee. Distributed fault-tolerant embedding of rings in hypercubes. *Journal of Parallel and Distributed Computing*, 11:63–71, 1991.

[14] C.C. Chang, H.Y. Chen, and C.Y. Chen. Symbolic Gray code as a data allocation scheme for two-disc systems. *The Computer Journal*, 35(3):299, 1992.

[15] M. Chen and K.G. Shin. Subcube allocation and task migration in hypercube machines. *IEEE Trans. Comput*, 39:1146–1155, 1990.

[16] X.B. Chen. Unpaired many-to-many vertex-disjoint path covers of a class of bipartite graphs. *Information processing letters*, 110:203–205, 2010.

[17] J. H. Clark, J. C. George, and T. D. Porter. On the number of 1-factors in the n-cube. *Congr. Numerantium*, 127:67–69, 1997.

[18] K. Day and A.E. Al-Ayyoub. Fault diameter of k-ary n-cube networks. *IEEE Transactions on Parallel and Distributed Systems*, 8(9):903–907, 1997.

[19] P. Diaconis and S. Holmes. Gray codes for randomization procedures. *Statistics and Computing*, 4(4):287–302, 1994.

[20] K. Diks and A. Pelc. Efficient gossiping by packets in networks with random faults. *SIAM Journal on Discrete Mathematics*, 9:7–18, 1996.

[21] D. Dimitrov, T. Dvořák, P. Gregor, and R. Škrekovski. Gray codes avoiding matchings. *Discrete Mathematics & Theoretical Computer Science*, 11(2):123–147, 2009.

[22] R. J. Douglas. Bounds on the number of Hamiltonian circuits in the n-cube. *Discrete Math.*, 17:143–146, 1977.

[23] T. Dvořák. Hamiltonian cycles with prescribed edges in hypercubes. *SIAM J. Discret. Math.*, 19(1):135–144, 2005.

[24] T. Dvořák and P. Gregor. Hamiltonian fault-tolerance of hypercubes. *El. notes in Disc. Math.*, 29:471–477, 2007.

[25] T. Dvořák and V. Koubek. Long paths in hypercubes with a quadratic number of faults. *Information Sciences*, 179:3763–3771, 2009.

[26] T. Dvořák and V. Koubek. On the complexity of finding long paths and cycles in faulty hypercubes. Submitted., 2009.

[27] S.F. Edwards and P.W. Anderson. Theory of spin glasses. *Journal of Physics F: Metal Physics*, 5:965–974, 1975.

[28] C. P. Egoryĉev. A solution of van der Waerden's permanent problem. *Dokl. Akad. Nauk SSSR*, 258:1041–1044, 1981.

[29] A.H. Esfahanian and S.L. Hakimi. Fault-tolerant routing in de Bruijn communication networks. *IEEE Transactions on Computers*, 100(34):777–788, 1985.

[30] D. I. Falikman. A proof of van der Waerden's conjecture on the permanent of a doubly stochastic matrix. *Mat. Zametki*, 29:931–938, 1981.

[31] C. Faloutsos. Gray codes for partial match and range queries. *IEEE Transactions on Software Engineering*, pages 1381–1393, 1988.

[32] W.C. Fang, C.C. Hsu, and C.M. Wang. On the fault-tolerant embeddings of complete binary trees in the mesh interconnection networks. *Information Sciences*, 151:51–70, 2003.

[33] T. Feder and C. Subi. Matchings and cycle decompositions in hypercubes. Submitted.

[34] T. Feder and C. Subi. Nearly tight bounds on the number of Hamiltonian cycles of the hypercube and generalizations. In *Electronic Colloquium on Computational Complexity*, number 063 in TR07, 2007.

[35] J. Fink. Perfect matchings extend to Hamilton cycles in hypercubes. *J. Comb. Theory, Ser. B*, 97(6):1074–1076, 2007.

[36] J. Fink. Connectivity of matching graph of hypercube. *SIAM J. Discrete Math*, 23:1100–1109, 2009.

[37] J. Fink. Matching graphs of hypercubes and complete bipartite graphs. *European J. Comb.*, 30:1624–1629, 2009.

[38] J. Fink. Towards a theory of ground state uniqueness. Technical Report 966, KAM-DIMATIA Series, Malostranské náměstí 25, 118 00 Praha 2, Czech Republic, 2010.

[39] J. Fink and P Gregor. Long cycles in hypercubes with optimal number of faulty vertices. Submitted, 2009.

[40] J. Fink and P. Gregor. Long pairs of paths in faulty hypercubes. Technical Report 465, Institute for Theoretical Computer Science, Charles University, Malostranské náměstí 25, 118 00 Praha 2, Czech Republic, 2009.

[41] J. Fink and P. Gregor. Long paths and cycles in hypercubes with faulty vertices. *Information Sciences*, 179:3634–3644, 2009.

[42] D.S. Fisher and D.A. Huse. Ordered phase of short-range Ising spin-glasses. *Physical review letters*, 56(15):1601–1604, 1986.

[43] M.E. Fisher. Statistical mechanics of dimers on a plain lattice. *Phys. Rev.*, 124:278–286, 1961.

[44] D.G. Fon-Der-Flaass. Extending pairings to Hamiltonian cycles. *Siberian Electronic Mathematical Reports*, 7:115–118, 2010.

[45] J.-S. Fu. Fault-tolerant cycle embedding in the hypercube. *Parallel Computing*, 29(6):821–832, 2003.

[46] J.-S. Fu. Longest fault-free paths in hypercubes with vertex faults. *Information Sciences*, 176(7):759–771, 2006.

[47] M. Gardner. The curious properties of the Gray code and how it can be used to solve puzzles. *Sci. American*, 227:106–109, 1972.

[48] F. Gray. Pulse code communication, 1953. US Patent 2,632,058.

[49] P. Gregor. Perfect matchings extending on subcubes to Hamiltonian cycles of hypercubes. *Discrete Mathematics*, 309:1711 – 1713, 2009.

[50] L. Gros. *Théorie du Baguenodier*. Aimé Vingtrinier, Lyon, 1872.

[51] A.K. Hartmann. How to evaluate ground-state landscapes of spin glasses thermodynamical correctly. *The European Physical Journal B-Condensed Matter and Complex Systems*, 13(3):539–545, 2000.

[52] S.-Y. Hsieh. Fault-tolerant cycle embedding in the hypercube with more both faulty vertices and faulty edges. *Parallel Computing*, 32(1):84–91, 2006.

[53] C.-N. Hung, Y.-H. Chang, and C.-M. Sun. Longest paths and cycles in faulty hypercubes. In *Parallel and Distributed Computing and Networks*, pages 101–110, 2006.

[54] E. Ising. Beitrag zur theorie des ferromagnetismus. *Zeitschrift fűr Physik A Hadrons and Nuclei*, 31(1):253–258, 1925.

[55] P. W. Kasteleyn. The statistics of dimers on a lattice : I. the number of dimer arrangements on a quadratic lattice. *Physica*, 27:1209–1225, 1961.

[56] D.S.S. Kirkpatrick and D. Sherrington. Solvable Model of a Spin-Glass. *Phys. Rev. Lett*, 35:1792–1796, 1975.

[57] D. E. Knuth. *The Art of Computer Programming*, volume 4, fascicle 2. Addison-Wesley, 2005.
See errata at http://www-cs-faculty.stanford.edu/~knuth/err4f2.textxt.

[58] V. Koubek, 2008. Private communication.

[59] G. Kreweras. Matchings and Hamiltonian cycles on hypercubes. *Bull. Inst. Combin. Appl.*, 16:87–91, 1996.

[60] T.-L. Kueng, T. Liang, L.-H. Hsu, and J.J.M Tan. Long paths in hypercubes with conditional node-faults. *Information Sciences*, 179:667–681, 2009.

[61] F.T. Leighton. *Introduction to parallel algorithms and architectures: array, trees, hypercubes*. Morgan Kaufmann Publishers Inc. San Francisco, CA, USA, 1991.

[62] M. Lewinter and W. Widulski. Hyper-hamilton laceable and caterpillar-spannable product graphs. *Computers & Mathematics with Applications*, 34(11):99–104, 1997.

[63] T.K. Li, J.J.M. Tan, and L.H. Hsu. Hyper hamiltonian laceability on edge fault star graph. *Information Sciences*, 165(1-2):59–71, 2004.

[64] A.C. Liang, S. Bhattacharya, and W.T. Tsai. Fault-tolerant multicasting on hypercubes. *Journal of Parallel and Distributed Computing*, 23(3):418–428, 1994.

[65] M. Loebl. Ground state incongruence in 2d spin glasses revisited. *Electr. J. Comb.*, 11(1), 2004.

[66] R.M. Losee Jr. A Gray code based ordering for documents on shelves: Classification for browsing and retrieval. *Journal of the American Society for Information Science*, 43(4):312–322, 1999.

[67] J. Ludman. Gray code generation for MPSK signals. *IEEE Transactions on Communications*, 29(10):1519–1522, 1981.

[68] M. Ma, G. Liu, and X. Pan. Path embedding in faulty hypercubes. *Applied Mathematics and Computation*, 192(1):233–238, 2007.

[69] W. L. McMillan. Cluster-quench simulation of the two-dimensional random Ising model. *J. Phys. C*, 17(18):3189–3193, 1984.

[70] M. Mezard, G. Parisi, and M.A. Virasoro. Spin glass theory and beyond. In *World scientific Singapore*, 1987.

[71] H. Minc. Upper bound for permanents of (0,1)-matrices. *Bull. Amer. Math. Soc.*, 69:789–791, 1963.

[72] C.M. Newman and D.L. Stein. Multiple states and thermodynamic limits in short-ranged Ising spin-glass models. *Physical Review B*, 46(2):973–982, 1992.

[73] C.M. Newman and D.L. Stein. Nature of ground state incongruence in two-dimensional spin glasses. *Physical review letters*, 84(17):3966–3969, 2000.

[74] C.M. Newman and D.L. Stein. TOPICAL REVIEW: Ordering and broken symmetry in short-ranged spin glasses. *Journal of Physics: Condensed Matter*, 15(32):R1319–R1364, 2003.

[75] A. Nijenhuis and H.S. Wilf. *Combinatorial algorithms: for computers and calculators*. Academic Press New York, 1978.

[76] M. Palassini and A.P. Young. Triviality of the ground state structure in Ising spin glasses. *Physical Review Letters*, 83(24):5126–5129, 1999.

[77] D. Richards. Data compression and Gray-code sorting. *Information Processing Letters*, 22(4):201–205, 1986.

[78] J.P. Robinson and M. Cohn. Counting sequences. *IEEE Transactions on Computers*, 30(1):17–23, 1981.

[79] F. Ruskey and C.D. Savage. Hamilton Cycles that Extend Transposition Matchings in Cayley Graphs of S_n. *SIAM Journal on Discrete Mathematics*, 6(1):152–166, 1993.

[80] C. Savage. A survey of combinatorial gray codes. *SIAM Review*, 39(4):605–629, 1997.

[81] A. Sengupta. On ring embedding in hypercubes with faulty nodes and links. *Information Processing Letters*, 68(4):207–214, 1998.

[82] C.-H. Tsai. Cycles embedding in hypercubes with node failures. *Information Processing Letters*, 102(6):242–246, 2007.

[83] Y.-C. Tseng. Embedding a ring in a hypercube with both faulty links and faulty nodes. *Information Processing Letters*, 59(4):217–222, 1996.

[84] A.N. Tychonoff. Uber die topologische erweiterung von raumen. *Mathematische Annalen*, 102(1):544–561, 1930.

[85] B.L. van der Waerden. Aufgabe 45. *Jber. Deutsch. Math.–Verein.*, 35:117, 1926.

[86] I.M. Wanless. Perfect factorisations of bipartite graphs and Latin squares without proper subrectangles. *Journal of combinatorics*, 6:135–150, 1998.

[87] G. Wiener. Edge multiplicity and other trace functions. In *Proceedings of European Conference on Combinatorics, Graph Theory and Applications (EuroComb 2007)*, volume 29 of *Electronic Notes in Discrete Mathematics*, pages 491–495, 2007.

[88] J. Wu. Safety levels-an efficient mechanism for achieving reliablebroadcasting in hypercubes. *IEEE Transactions on Computers*, 44(5):702–706, 1995.

[89] J. Xu. *Topological structure and analysis of interconnection networks*. Springer Netherlands, 2001.

[90] J.-M. Xu and M. Ma. Survey on path and cycle embedding in some networks. *Frontiers of Mathematics in China*, 4:217–252, 2009.

[91] P.J. Yang, S.B. Tien, and C.S. Raghavendra. Embedding of rings and meshes onto faulty hypercubes using free dimensions. *IEEE Transactions on Computers*, 43:608–613, 1994.