Karlsruher Institut für Technologie

Bachelorthesis

On the Resolution of the Sensitivity Conjecture

David Schuldes

06.04.2021

At the Department of Informatics
Institute of Theoretical Informatics, Algorithm Engineering

1st Reviewer: PD Dr. Torsten Ueckerdt
2nd Reviewer: Prof. Dr. Peter Sanders
Advisor: PD Dr. Torsten Ueckerdt

Abstract

The sensitivity of a boolean function is defined as the maximum number of indices of any input vector $x \in \{0,1\}^n$ such that flipping the input vector at the index changes the value of $f(x)$. The Sensitivity Conjecture states that for every boolean function $f : \{0,1\}^n \to \{0,1\}$ the sensitivity is at most polynomially smaller than another complexity measure of f, the so-called block sensitivity. Although appearing trivial at first sight, this conjecture has stood as one of the most frustrating open problems in all of combinatorics and theoretical computer science since it was proposed by Nisan and Szegedy in 1989. Recently, Hao Huang, a mathematician at Emory University, has posted a 6-page preprint that finally proves the Sensitivity Conjecture. In this thesis we will explore the proof and make use of the techniques used by Hao Huang in order to gain further structural insights on the relationship between a special group of matrices and its corresponding induced graphs. Moreover, we will gain additional insight in the structure of induced subgraphs of the n-dimensional hypercube.

Zusammenfassung

Die Sensitivity Conjecture besagt, dass für eine bool'sche Funktion $f : \{0,1\}^n \to \{0,1\}$ die so genannte sensitivity, also maximale Anzahl der indizes für die sich bei einem beliebigen, festen Argument Vektor der Funktionswert $f(x)$ ändert, wenn der sich einzelne index ändert, höchstens polynomiell geringer als ein anderes Komplexitätsmaß, namentlich die so genannte Block Sensitivity ist. Obwohl diese Vermutung auf den ersten Blick trivial erscheinen mag hat sich sich als eines der frustrierensten ungelösten Probleme im Themengebiet der Kombinatorik und Graphentheorie erwiesen seitdem sie 1989 von Nisan und Szegedy aufgestellt wurde. Vor kurzem hat Hao Huang, ein Mathematiker der Emory University einen Sechsseitigen Beweiß der Sensitivity Conjecture veröffentlicht. In dieser Arbeit untersuchen wir die Herangehensweise und Techniken dieses Beweises und nutzen letztere um weitere strukturelle Einsichten bezüglich des Verhältnisses zwischen einer Matrizenklasse und den von ihr induzierten Graphen zu gewinnen. Außerdem werden wir weitere strukturelle Erkenntnis über den n-Hyperwürfel gewinnen.

Contents

1 Introduction and Motivation

A function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is called a boolean function. Boolean functions first occurred in the mathematical formulation of logical problems, and were named after G. Boole, who laid the foundation for the applications of mathematics in logic in the 19th century. Boolean functions play a fundamental role in the design of digital circuits and chips used for computers where they are used to model the behaviour of a circuit system. The properties of boolean functions are critical in cryptography, particularly in the design of symmetric key algorithms.

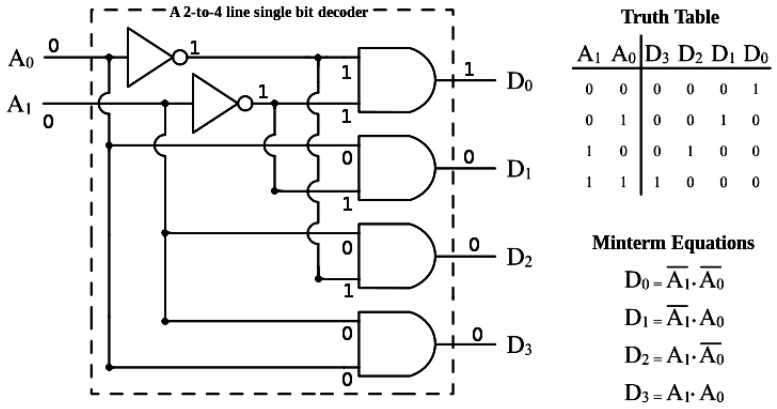


Figure 1: An abstract representation of digital circuit functions via a boolean function.

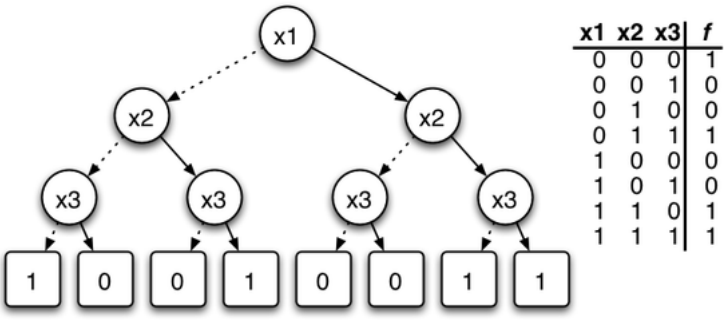


Figure 2: A binary decision tree and its corresponding boolean function

In 1989, mathematicians Noam Nisan and Mario Szegedy proposed the Sensitivity Conjecture [10]. It proposes a polynomial lower bound between two different measures of complexity of a boolean function. Ever since then the Sensitivity Conjecture had remained to be an apparently trivial yet unproven problem within all of combinatorics and theoretical computer science. Other seemingly similar conjectures were proven with

relative ease whilst a number of very reputable people within the field tried unsuccessfully to prove the Sensitivity Conjecture. In August 2019, a mathematician from Emory University by the name of Hao Huang published a 6-page paper that proves the Sensitivity Conjecture by utilizing methods from both spectral graph theory and eigenvalues of matrices in a manner not discerned beforehand [8]. In this thesis we inspect Huangs methodology and try to infer further use for both the tools of spectral graph theory he employed as well as the main theorem of his paper.
In the subsequent section, we will explore the concepts of boolean functions, eigenvalues of matrices and spectral graph theory, as well as theorems from the respective fields, that Huang draws from for his proof.

2 Preliminary Definitions and Theorems

2.1 Introduction to boolean functions

A function $f : \{0,1\}^n \longrightarrow \{0,1\}$ is called a boolean function. It is common practice to interpret the value 0 as false and the value 1 as true. Examples of frequently used functions are the logical AND function f_{AND} in n *variables.* $f(x_1, ..., x_n) = 1$ if and only if $x_1 = ... = x_n = 1$ it can be interpreted as the logical conjunction of $x_1, ..., x_n$. Boolean functions realizing the logical OR f_{OR} are constructed according to the same principle, so for instance $f_{OR}(x_1, ..., x_n) = 0$ if and only if $x_1 = ... = x_n = 0$. These basic boolean functions may be utilized as building blocks for modeling more complex behaviour. Among the most prominent instances of example are disjunctive and conjunctive normal forms respectively.
In boolean logic, a disjunctive normal form (DNF) is a canonical normal form of a logical formula consisting of a disjunction of conjunctional clauses. A conjunctional clause of boolean variables $x_1, ..., x_n$, i.e. variables whose value is either true or false or in our case, 0 or 1, can be thought of as $f_{AND}(x_1, .., x_n)$. In other words, a DNF can be viewed as an f_{OR} function where its argument vector consists of a set of f_{AND} functions both of which we have just introduced. More formally, let $x_1 \wedge ... \wedge x_n$ denote $f_{AND}(x_1, ..., x_n)$, then a disjunctive normal form may be $(x_1 \wedge x_2 \wedge x_3) \vee (x_4 \wedge x_5) = f_{OR}(f_{AND}(x_1, x_2, x_3), f_{AND}(x_4, x_5))$. Analogously, a conjunctive normal form (KNF) is a conjunction of one or more disjunctional clauses. As a canonical normal form, it is useful in automated theorem proving and circuit theory and arguably of even greater importance than DNF's since KNF's are of central interest to the boolean satisfiability problem.
In logic and computer science, the Boolean satisfiability problem (sometimes abbreviated SATISFIABILITY or SAT) is the problem of determining if there exists an interpretation that satisfies a given KNF boolean formula. In other words, it asks whether the variables of a given boolean formula can be consistently replaced by the values TRUE or FALSE in such a way that the formula evaluates to TRUE. SAT is the first problem that was proven to be NP-complete [4]. This means that all problems in the complexity class NP, which includes a wide range of natural decision and optimization problems, are at most as difficult to solve as SAT and more importantly can be transformed into a KNF that, if solveable, yields a solution to the problem originally at hand.
When studying boolean functions, it is of interest to examine the behaviour of a given boolean function f when its argument vector $x \in \{0,1\}^n$ changes. One approach towards measurement of the changing behaviour of a boolean function f with respect to its argument $x = (x_1, ..., x_n)$ is its so-called *sensitivity.* In order to introduce the concept of sensitivity, we must first make a number of definitions imperative to its introduction. Let $S \subset \{1, ..., n\}$ be a subset. In the following, the elements of S will be interpreted as index of the argument vectors $x \in \{0,1\}^n$ of a given boolean function $f : \{0,1\}^n \to \{0,1\}$. Given an argument vector x of a boolean function $f : \{0,1\}^n \to \{0,1\}$ and an index $i \in \{1, ..., n\}$, then we define $x^i = (x_1, ..., (1 - x_i), ..., x_n)\}$ in other words, x^i denotes the boolean vector arising from the original vector x by only flipping index i. The

local sensitivity of f with regard to x, written as $s(f,x)$ denotes the number k of indices $\{i_1,...,i_k\}$ so that $f(x^{i_m}) \neq f(x)$ for $m \in \{1,...,k\}$. For the sake of clarification, this number must obviously be uniquely determined. The sensitivity of f is defined as $s(f) := \max\{s(f,x) \mid x \in \{0,1\}^n\}$. If $s(f,x) = 5$ for a boolean function f, then there exists an argument vector x and a set $S = \{i_1,...,i_5\}$, such that $f(x) \neq f(x^{i_k})$ for $k \in \{1,...,5\}$.
A measure of complexity closely related to sensitivity is the so-called of block sensitivity. In order to define block sensitivity, we need to introduce another concept. Given $S \subset \{1,...,n\}$, x^S denotes the argument vector that is obtained by flipping all indices $\{i_1,...,i_k\} = S$ in x. As an example, suppose $x = (0,1,0,1,0)$ and $S = \{2,5\}$ then $x^S = (0,0,0,1,1)$. Now, consider a set $\tilde{S} = \{S_1,...,S_k\}$ containing subsets of indices as described before. The subsets are pairwise disjoint which means $S_i \cap S_j = \emptyset$ if $i \neq j$ for any $i,j \in \{1,...,k\}$. The *block sensitivity* of f with regard to x, $bs(f,x)$ is the maximum number k of pairwise disjoint subsets of indices $S_1,...,S_k \subset \{0,1\}^n$ such that $f(x^{S_j} \neq f(x)$ for $S_j \in \{S_1,...,S_k\}$. The block sensitivity of f, $bs(f)$ is defined analogously as sensitivity, $bs(f) := \max\{bs_x(f) \mid x \in \{0,1\}^n\}$. We can think of block sensitivity as an analogue to sensitivity. While the latter concept is concerned with the sole index of an input vector, in block sensitivity the analogue is a set of indices rather than just one index. Keeping this in mind and by considering the partition where every B_i is a singleton (i.e. every B_i contains exactly one element), we see that block sensitivity is at least as large as sensitivity, so $s(f) \leq bs(f)$.
For some classes of boolean functions, $s(f) = bs(f)$ holds. In order to see this, we introduce the concepts of monotonic boolean functions and certificate complexity. Let $a,b \in \{0,1\}^n$. A monotonic function is one such that for all a_i and b_i, if $a_1 \leq b_1$, $a_2 \leq b_2$, ..., $a_n \leq b_n$, then $f(a_1,...,a_n) \leq f(b_1,...,b_n)$. In other words, a Boolean function is monotonic if and only if, for every combination of inputs, switching one of the inputs from false to true can only cause the output to switch from false to true and not from true to false. A third measurement of complexity of a boolean function f is the so called certificate complexity $C(f)$. A *1-certificate* (or *0-certificate*) for f is an assignment to a subset of the variables so that the output of f is forced to 1 (or 0) in other words, any change in a variable that is not included in the subset may change whilst the output value will not change. For any input x, $C_x(f)$ denotes the size of the smallest certificate, so that the value of f with this certificate is equal to that of $f(x)$. The *certificate complexity* $C(f)$ is the maximum of $C_x(f)$ for all $x \in \{0,1\}^n$. In more prosaic terms, the certificate complexity of a function describes how many input bits must be revealed in order to determine the output value of that function on every input. Now, clearly $bs(f) \leq C(f)$ for any boolean function f because in every for $bs(f,x)$ and any B_i, there is as least one index that must belong to the certificate of f. Otherwise, $f(x^{B_i}) = f(x)$.
As mentioned before, $s(f) = bs(f)$ for a class of boolean functions, namely all monotonic boolean functions. In order to understand this, we simply prove $C(f) \leq s(f)$. Let's consider any monotonic function f. Let x be the input string with $C_x(f) = C(f)$. Without loss of generality, we assume $f(x) = 1$. Every index of x that counts towards the certificate must change the value of $f(x)$ if it is flipped. Because f is monotonic, any change of a variable from 1 to 0 can only result in an output change from 1 to

0, but $f(x) = 1$. Therefore, every variable in the certificate must have value 1. Now $C(f) \leq s(f)$ so $s(f) \leq bs(f) \leq C(f) \leq s(f)$ yields our desired claim, $s(f) = bs(f)$. The sensitivity conjecture postulates the question, whether the lower bound for $s(f) \leq bs(f)$ is polynomial in $s(f)$. Two measures of complexity, in our case $s(f)$ and $bs(f)$, are said to be *polynomially related* if there exist polynomials $p_1(x)$ and $p_2(x)$ such that for every boolean function f $s(f) \leq p_2(bs(f))$ and $bs(f) \leq p_1(s(f))$ holds. Boolean functions may be represented as a real polynomial, too. Let $v \in \{0,1\}^n$ be a boolean vector, we define the multilinear polynomial $P_v(x) : \mathbb{R}^n \to \mathbb{R}$ as follows. $P_v(x) := \prod_{i \in B} x_i \cdot \prod_{j \in \overline{B}} (1 - x_j)$ where $i \in B \leftrightarrow x_i = 1$ and $j \in \overline{B} \leftrightarrow x_j = 0$. The polynomial has the property that it $P_v(x) = 0$ if $x \neq v$ and $P_v(v) = 1$. This polynomial has degree n where the coefficient of the term $v_1 \cdot v_2 \cdot ... \cdot v_n$ is either $+1$ or 1 depending on the parity of v. A polynomial $p : \mathbb{R}^n \to \mathbb{R}$ represents a boolean function f if for all $x \in \{0,1\}^n$ $p(x) = f(x)$. Every boolean function can be represented as sum of polynomial functions as follows: $P_f = \sum_{v:f(v)=1} P_v$.

This connection is used in Huang's proof. For a boolean function f, $deg(f)$ denotes the maximum degree of the real polynomial that represents f. Now, since we have introduced the concepts necessary for grasp of the postulated Sensitivity Conjecture, we will finally explore its sentiment.

Theorem 1. *There exists an absolute constant $C > 0$, such that for every boolean function f we have $bs(f) \leq s(f)^C$.*

Boolean functions may be represented by polynomials. For a boolean function f we let $deg(f)$ denote the degree, in other words the exponent of highest order, of the polynomial representing f. The following theorem was established by Tal [3].

Theorem 2 (Tal)**.** *For any boolean function f, $bs(f) \leq deg(f)^2$.*

2.2 Modular arithmetic and groups

We need to introduce modular arithmetic because it will be used in a number of proofs. For $a, b, m \in \mathbb{Z}$, $a \equiv b \mod m \leftrightarrow m \mid (a - b) \leftrightarrow \exists k \in \mathbb{Z} : k \cdot m = (a - b)$ Obviously, if $a \equiv b \mod m$, then $m \mid (a - b) = (a + r) - (b + r)$, so $a + r \equiv b + r \mod m$. Group theory will be of importance when we will examine related works that build upon the main theorem of Hao Huang. A group G is a non-empty set with a binary operation $\cdot : G \times G \to G$, $\cdot(g_1, g_2) \mapsto g_1 \cdot g_2$ that satisfies the following three group axioms. For $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$. There exists an element $e_G \in G$ so that for $a \in G$ $a \cdot e_G = e_G \cdot a = a$. For each $a \in G$ there exists $a^{-1} \in G$ so that $a \cdot a^{-1} = a^{-1} \cdot a = e_G$. A subgroup $H \subset G$ is a subset that is also a group so in other words, it fulfills the three group axioms. A subgroup N is said to be a normal subgroup if it is invariant under conjugation. That is, for all $g \in G$ $g \cdot N \cdot g^{-1} \subset N$. This is important because normal subgroups are used to define quotient groups which in turn are needed to establish a theorem on the relation of special mappings between groups. Let N be a normal

subgroup of G, define $G_N := \{g \cdot N \mid g \in G\}$ and $g_1N \cdot g_2N := (g_1 \cdot g_2)N$. Because N is a normal subgroup this binary operation is well defined and allows to define the quotient group G_N. It is left to the diligent reader to reassure himself or herself, that the quotient group also fulfills all three group axioms and is in fact a group. A group homomorphism is a mapping $\Phi : G \to H$ between two groups $(G, \cdot)$ and $(H, \star)$ so that $\Phi(g_1 \cdot g_2) = \Phi(g_1) \star \Phi(g_2)$ for all $g_1, g_2 \in G$. The kernel of a group homomorphism is defined as follows, $ker(\Phi) := \{g \in G \mid \Phi(g) = e_H\}$. Every kernel of a homomorphism Φ is a normal subgroup, $\Phi(g) \star \Phi(k) \star \Phi(g^{-1}) = \Phi(g) \star e_H \star \Phi(g^{-1}) = \Phi(e_G) \in ker(\Phi)$ for all $g \in G, k \in ker(\Phi)$. This allows us to define $G_{ker(\Phi)}$ and $\tilde{\Phi} : G_{ker(\Phi)} \to image(\Phi)$, $\tilde{\Phi}(gN) := \Phi(g)$ which is a bijection. This result is also called the fundamental theorem on homomorphisms, in other words $G_{ker(\Phi)} \cong image(\Phi)$ and $\frac{|G|}{|ker(\Phi)|} = | \ image(\Phi) \ |$ if G is finite. We will make use of this equation in Chapter 4.

2.3 Introduction to graph theory

Drawing away from boolean functions, we will now occupy ourselves with some basic structures and notions of graph theory, the second field of mathematics that is being touched upon by Huangs proof.
In the field of graph theory, a *bipartite graph* is a graph whose vertices can be divided into two disjoint and independent sets U and V such that every edge connects a vertex in U to one in V. The graph $K_{m,n}$ denotes the complete bipartite graph where U consists of m nodes and V consists of n nodes and every vertex in U is connected by an edge to each vertex in V. So in $K_{1,n}$ for instance, there exists one node in U which is connected to every node in V whilst no two nodes within V are connected. For further use in our proofs, we introduce some concepts drawn from modular arithmetic and prove the following lemma

Lemma 2.1. *A graph $G = (V, E)$ is bipartite if and only if it has no odd cycle (a cycle is odd if it contains an even number of vertices).*

Proof. " $\rightarrow$ " We assume our given graph $G = (V, E)$ is bipartite and we have partitioned the node set V into two disjoint partition classes U, W. Suppose there exists an odd cycle C in G. Starting at an arbitrary node v_1 on C, any two adjacent nodes must lie within different bipartition classes. We label the nodes alternatingly 1 if they lie within U and 2 if they lie in W, without loss of generality we assume v_1 lies within U . But since C is odd, there is an even number of nodes so at the end of one iteration over all nodes the starting node is labeled 2. This contradicts our premise.
" $\leftarrow$ " We assume there does not exist an odd cycle in G. As we shall find out, this is already sufficient to construct a bipartite partition on the node set of G. In order to stay consistent with our prior notation, let the two disjoint sets of partition classes be denoted by U and V. We pick an arbitrary starting node v_1 in G and without loss of generality whilst adhering to our technique of labeling, we label v_1 with 1 denoting that v_1 lies within partition U. Now, clearly all of v_1's neighbour nodes $v_2, ..., v_k$ must lie within V which which forces us to assign them with label 2. Now, we inductively

continue the labeling of neighbour nodes process on each of $v_2, ..., v_k$. There may exist cycles within the graph. Without loss of generality let $c_1, ..., c_k$ denote the sequence of adjacent nodes on the cycle. Since we assume that there do not exist odd cycles in G and every even cycle consists of an uneven number of nodes, $k \equiv 0 \mod 2$. This means, that it is possible to assign an alternating labeling on $c_1, ..., c_k$. Since any path in G can obviously be labeled alternatingly and any cycle can be labeled alternatingly as well as we just argued, the labeling induces a bipartite partitioning where every node labeled with 1 is assigned to the partition class U and every node labeled with 2 therefore must be assigned to partition class V. □

For his proof of the Sensitivity Conjecture, Huang links the concept of (block)-sensitivity of a boolean function to the n-hypercube, a well known structure in graph theory that we will familiarize ourselves with in the following.
For $n \in \mathbb{N}$, the *n-hypercube* Q_n is defined as the set V of 2^n nodes represented by coordinate vectors $V := \{0,1\}^n$. Two nodes are adjacent if and only if their coordinate vectors differ in exactly one coordinate. Inductively, the $(n+1)$-hypercube can be obtained algebraically from an n-hypercube by increasing the dimension of the node set from 2^n to 2^{n+1}. Since this induces a new edge for every set of two nodes that differ only in coordinate $n+1$, we can imagine this procedure geometrically as "cloning" the n-hypercube and connecting the cloned nodes within the two hypercubes by an edge. The figure below serves as illustration. This frame of thought about the inductive construction makes for an accessible intuition about objects in spaces of dimensions larger than 3.
The hypercube graph Q_n may be constructed from the family of subsets of a set with n elements, by making a vertex for each possible subset and joining two vertices by an edge whenever the corresponding subsets differ in a single element. Equivalently, it may be constructed using $2n$ vertices labeled with n-bit binary numbers and connecting two vertices by an edge whenever the Hamming distance of their labels is one. The Hamming distance between two strings of equal length is the number of positions at which the corresponding symbols are different. In other words, it measures the minimum number of substitutions required to change one string into the other. These two constructions are closely related: a binary number may be interpreted as a set (the set of positions where it has a 1 digit), and two such sets differ in a single element whenever the corresponding two binary numbers have Hamming distance one.
Additionally, every hypercube Q_n with $n > 1$ has a Hamiltonian cycle, a cycle that visits each vertex exactly once. We can inductively construct such a cycle by using the algebraic notion of Q_n. Given a Hamiltonian Cycle for the $n-1$-hypercube $(0, ..., 0), (0, ..., 0, 1)...(1, 0, ..., 0), (0, ..., 0)$ we construct a Hamiltonian cycle for the n-hypercube as follows. $(0, ..., 0, 1), (0, ..., 0, 1, 1)...(1, 0, ..., 0, 1), (1, 0, ..., 0)...(0, ..., 0, 1, 0)$, $(0, ..., 0), (0, ..., 0, 1)$.

Now, we will collect a number of properties of Q_n that we will utilize throughout this

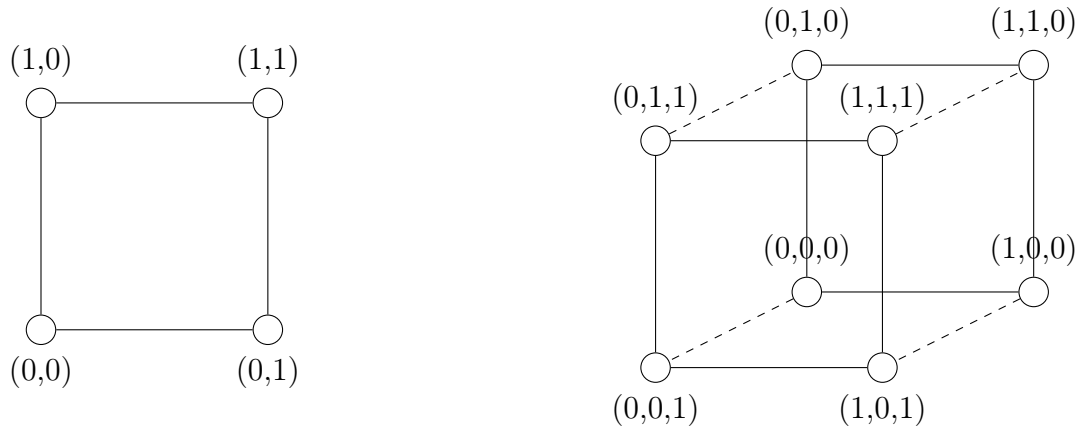


Figure 3: Geometric expansion of Q_2 to Q_3.

thesis as tools for further proofs. Since every node is connected to exactly n other nodes we can determine the number of edges within Q_n by counting the number of edges for every node and dividing by *two* since we counted every edge twice. Overall there exist $\frac{n \cdot 2^n}{2} = n \cdot 2^{n-1}$ edges in Q_n.
Another important concept within graph theory is that of an independent set. It denotes a set of vertices in a graph, no two of which are adjacent. In other words, a set S of vertices such that for every two vertices in S, there is no edge connecting the two. Equivalently, each edge in the graph has at most one endpoint in S. The size of an independent set is the number of vertices it contains. A *maximum independent set* is an independent set of largest possible size for a given graph G. This size is called the independence number of G, and denoted $\alpha(G)$. The problem of finding such a set is called the maximum independent set problem and is an *NP-hard optimization problem.* For now, we will claim that the size of a maximum independent set in Q_n is 2^{n-1}. As we shall find out, a tool which Huang uses for his proof also yields a simple argument as to why our claim must be true.

Lemma 2.2. *Q_n is bipartite for $n \in \mathbb{N}$.*

Proof. Suppose for the sake of contradiction that C is an odd cycle in Q_n. We pick an arbitrary vertex v_1 as start-vertex and without loss of generality assume $v_1, ..., v_k$ to denote the sequence of nodes on C, meaning that v_1 is adjacent to v_2 and v_k. We define $d(u, v)$ to be the number of indices that differ in the algebraic notation of any two vertices from Q_n. In Q_4 for instance $d((0, 1, 1, 0), (1, 0, 1, 0)) = 2$. Since adjacent nodes differ in exactly one coordinate $d(v_1, v_{n+1}) = d(v_1, v_n) + 1$ and since $d(v_1, v_2) = 1$ we get $d(v_1, v_n) \equiv n - 1 \mod 2$. Remember, that v_k denotes the last node on C in our labeling sequence and that v_1 is adjacent to v_k. Since C is an odd cycle, there is an odd number of vertices so $k \equiv 1 \mod 2$ and thus $d(v_1, v_k) \equiv n - 1 \mod 2 \equiv 0 \mod 2$. Since $v_1 \neq v_k$ this would mean that both nodes differ in at least two coordinates and cannot be adjacent. Again, this contradicts our premise.
This proves our lemma. □

2.4 A little bit of Linear Algebra

In his proof of the Sensitivity Conjecture, Huang draws from methods of spectral graph theory that were not utilized beforehand and were presumably overlooked but are of central importance to the simplicity of Huangs chain of reasoning. In this section we will briefly explore the field of linear algebra which is a necessary preparation in order to understand the tools of spectral graph theory forming the backbone of Huangs proof. We will touch upon spectral graph theory afterwards and arguably more importantly even, we will make additional observations to Huangs findings yielding a greater insight about the relationship between the maximum degree of a graph and the eigenvalues of a matrix representing the structure of this graph.
A *matrix* $A \in \mathbb{R}^{n \times n}$ is a rectangular array comprised of n rows and n columns which have real numbers as entries.
A *submatrix* B of A is a matrix that is obtained by removing the same number of both rows and columns from the original matrix A. A principal submatrix is obtained by removing only both row and columns with the same index $i \in \{1, ..., n\}$. This procedure is exemplarily illustrated below in Figure 4.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \qquad\qquad \begin{pmatrix} 1 & 3 \\ 7 & 9 \end{pmatrix}$$

Figure 4: Construction of a principal submatrix.

The trace of a quadratic matrix $A \in \mathbb{R}^{n \times n}$ is defined as the sum of its diagonal elements. $tr(A) := \sum_{i=1}^{n} a_{i,i}$.
For any matrix $A \in \mathbb{R}^{n \times m}$, A^T denotes the matrix arising from A by transposing rows to columns. In other words, $a_{i,j} = a_{j,i}^T$ for every $i \in \{1, ..., n\}$ and $j \in \{1, ..., m\}$. A matrix $A \in \mathbb{R}^{n \times n}$ is symmetric if $A^T = A$. The figure below illustrates the transposition of a non-symmetric matrix.

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix} \qquad\qquad \begin{pmatrix} 1 & 4 & 7 \\ 2 & 5 & 8 \\ 3 & 6 & 9 \end{pmatrix}$$

(a) Exemplary matrix A (b) A^T arising from A

Let $A \in \mathbb{R}^{n \times m}$ denote an $n \times m$ matrix with entries in $\mathbb{R}$. An *eigenvector* of A is a vector $0 \neq v \in \mathbb{R}^n$, such that there exists $\lambda \in \mathbb{R}$ with $A \cdot v = \lambda \cdot v = (\lambda \cdot v_1, ..., \lambda \cdot v_n)^T$

where $\lambda \in \mathbb{R}$ is called *eigenvalue* of A to the eigenvector v.

$$\begin{pmatrix} -2 & -4 & 2 \\ -2 & 1 & 2 \\ 4 & 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 2 \\ -3 \\ -1 \end{pmatrix} = \begin{pmatrix} 6 \\ -9 \\ -3 \end{pmatrix} = 3 \cdot \begin{pmatrix} 2 \\ -3 \\ -1 \end{pmatrix}$$

A set of vectors $\{v_1, ..., v_n \mid v_i \in \mathbb{R}^n\}$ is said to be *linearly independent*, if the following statement holds, $\sum_{i=1}^{n} \lambda_i \cdot v_i = 0 \rightarrow \lambda_i = 0 \ \ \forall i \in \{1, ..., n\}$. A set of vectors $\{b_1, ..., b_n\} \subset V$ is said to *span a vectorspace* V if any vector $v \in V$ can be written as $\sum_{i=1}^{n} \lambda_i \cdot b_i$ for some $\lambda_i \in \mathbb{R}$.
For any given matrix $A \in \mathbb{R}^{n \times m}$, there may exist a set of linearly independent vectors $\{v_1, ..., v_k\} \in \mathbb{R}^n$, $u \neq v$ to the same eigenvalue. The matrix

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

has eigenvectors $\{(1, 0, 0)^T, (0, 1, 0)^T\}$ for the eigenvalue $\lambda = 2$. The *geometric multiplicity* of an eigenvalue λ with respect to a matrix A is defined as the *maximum number* of linearly independent vectors that span $E_\lambda := \{v \in \mathbb{R}^n \mid (A - \lambda I_n) \cdot v = 0\}$ where I_n denotes the identity matrix with n rows and columns. We can convert the equation $\{v \in \mathbb{R} \mid (A - \lambda I_n) \cdot v = 0\} = \{v \in \mathbb{R} \mid A \cdot v = (\lambda \cdot I_n) \cdot v\}$. Now it should be apparent, that this denotes the set of all eigenvectors to the eigenvalue λ.
In the proof of the Sensitivity Conjecture, the subsequent theorems about matrices and their respective eigenvalues are used.

Theorem 3. *Let $A \in \mathbb{R}^{n \times n}$ be symmetric. Then A has exactly n linearly independent eigenvectors $\{v_1, ..., v_n\}$.*

There do not necessarily exist n distinct eigenvalues, the following matrix has eigenvectors only to the same eigenvalues.

$$\begin{pmatrix} 2 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$$

Theorem 4 (Cauchys Interlace Theorem)**.** *Let A be a symmetric $n \times n$ matrix and B be a $m \times m$ principal submatrix of A, for some $m < n$. If the eigenvalues of A are $\lambda_1 \geq ... \geq \lambda_n$ and the eigenvalues of B are $\mu_1 \geq ... \geq \mu_m \in \mathbb{R}$, then for all $1 \leq i \leq m$, $\lambda_i \geq \mu_i \geq \lambda_{n-m+i}$.*

2.5 Spectral graph theory

Now that we have introduced the heralded mandatory concepts of linear algebra, we will briefly dive into a bit of spectral graph theory.
Spectral graph theory is concerned with the study of the properties of a graph in relationship with the eigenvalues and eigenvectors of matrices associated with this graph such as its adjacency matrix. In graph theory and computer science, an adjacency matrix is a square matrix used to represent a finite graph. The elements of the matrix indicate whether pairs of vertices are adjacent or not in the graph. In the special case of a finite simple graph, the adjacency matrix is a (0,1)-matrix with zeros on its diagonal. If the graph is undirected, the adjacency matrix is symmetric. Let $G = (V, E)$ be an undirected graph. We will construct a symmetric adjacency matrix representing the structure of G. First, we label every node in G from 1 to n. Then, we construct a *symmetric* matrix $A \in \{0,1\}^{n\times n}$ where $|V| = n$. Each row i and column i within A represents the node numbered i from G. Entries of A represent the edges within G. We set $a_{i,j} = 1$ if and only if the nodes i and j are adjacent in G.
For instance, there is an eigenvalue bound for independent sets in *regular graphs*, originally due to Alan J. Hoffman and Philippe Delsarte [7]. A *k-regular graph* is a graph where every node has exactly k *neighbours*. The bound is postulated as follows,

Theorem 5. *Suppose G is a k-regular graph on n vertices with its lowest eigenvalue λ_{min}, then*

$$\alpha(G) \leq \frac{n}{1 - \frac{k}{\lambda_{min}}}.$$

Coincidentally, Q_n is an *n-regular* graph. In his paper, Hao Huang utilized methods from spectral graph theory to prove the Sensitivity Conjecture which had been overlooked beforehand.

As pointed out beforehand, Huang draws from a tool of spectral graph theory. Even more so, his line of argument may be seen as building a bridge between boolean functions, Q_n and spectral graph theory. The following theorem is arguably of central importance to and perhaps main reason of his linking of these two fields. Therefore, we will explore the nature of reasoning behind the equivalence of the seemingly unrelated statements below. For the line of argument to function, we will use $C^n = \{-1, 1\}^n$ as the algebraic notation for nodes in Q_n and any boolean functions are consequently defined on C^n, $f : \{-1, 1\}^n \to \{-1, 1\}$.

Theorem 6 (Gotsman and Linial [6])**.** *The following are equivalent for a monotonic increasing function $h : \mathbb{N} \longrightarrow \mathbb{R}$.*

1. *For any induced subgraph H of Q_n with $|V(H)| \neq 2^{n-1}$, we have*

$$\max\{V(H), Q_n \setminus V(H)\} \geq h(n).$$

2. For any boolean function f, we have

$$s(f) \geq h(deg(f))$$

Proof. First, we will transform statements 1 and 2 into equivalent ones $1'$ and $2'$ and then show the equivalence of $1'$ and $2'$. Throughout this proof, we make use of the unique representation of f as a real polynomial over the cube, $f(x) = \sum_{I \subset \{1,...,n\}} (\alpha_I \cdot \prod_{i \in I} x_i)$, for all $I \subset \{1, ..., n\}$, $-1 \leq \alpha_I \leq 1$ holds. We define $\tilde{f}(I) := \alpha_I$ and let $deg(f)$ denote the degree of the polynomial representing f, so in other words
$deg(f) := \max\{\mid I \mid : \alpha_I \neq 0, I \subset \{1, ..., n\}\}$.
Now, onto the transformation of statements 1 and 2. Let $G = (V(G), E(G))$ be an arbitrary vertex induced subgraph of C^n and $g : \{-1, 1\}^n \to \{-1, 1\}$ a boolean function such that $g(x) = 1$ if and only if $x \in V(G)$. Then clearly, for the degree of any node $x \in V(G)$, $deg_G(x) = n - s(g, x)$ and the same holds in $C^n - G$ for any node $y \notin V(G)$. Now we define $\mathbf{E}(g)$ to be the average value of g on C^n. We postulate

1': For any boolean function g, $\mathbf{E}(g) \neq 0 \to \exists x : s(g, x) \leq n - h(n)$.
2': For any boolean function f, $s(f) < h(n) \to deg(f) < n$.

We show $1 \Rightarrow 1'$: assume 1 and assume that $\mathbf{E}(g) \neq 0$, this is equivalent to $\mid V(G) \mid \neq 2^{n-1}$ and because of our assumption 1 now $\max\{V(G), C^n \setminus V(G)\} \geq h(n)$ holds, which means that there exists a node x within G or $C^n \setminus G$ with $deg_G(x) \geq h(n)$. We have argued that $deg_G(x) = n - s(g, x)$ so we conclude, that $s(g, x) \leq n - h(n)$.
Now onto $1' \Rightarrow 1$: we assume for g, $\mathbf{E}(g) \neq 0 \to \exists x : s(g, x) \leq n - h(n)$ and $\mid V(G) \mid \neq 2^{n-1}$. The former is equivalent to $\mathbf{E}(g) \neq 0$ so $\exists x : s(g, x) \leq n - h(n) \leftrightarrow h(n) \leq n - s(g, x)$ holds and because $deg_G(x) = n - s(g, x)$ we conclude that $\max\{V(G), C^n \setminus V(G)\}$. Now onto the proof of $2 \to 2'$: we assume 2 and $s(f) < h(n)$ so $h(deg(f) < h(n)$ since h is monotonic increasing, $deg(g) < n$. Assuming $2'$, if $s(f) \geq h(deg(f))$ then since $deg(f) \leq n$ $s(f) = h(n)$ so $2'$ will always hold true.
Now to show $1' \Leftrightarrow 2'$: we define $g(x) := f(x) \cdot p(x)$ where $p(x) = \prod_{i=1}^{n} x_i$ is the parity function, so $p(x) = 1$ if there is an even number of indices such that $x_i = -1$ in x. Then we observe, that for all $x \in C^n$ $s(g, x) + s(f, x) = n \leftrightarrow s(g, x) = n - s(f, x)$ so for any $I \subset \{1, ..., n\}$, $\tilde{g}(I) = \tilde{f}(\{1, ..., n\} \setminus I)$, and since according to our definition, $\mathbf{E}(g) = \tilde{g}(\emptyset) = \tilde{f}(\{1, ..., n\} \setminus \emptyset)$, $\mathbf{E}(g)$ is the highest coefficient of the polynomial representing f. We assume $1'$ and $deg(f) = n$. Since this means $\mathbf{E}(g) = \tilde{f}(\{1, ..., n\}) \neq 0$ so because of $1'$, there exists an x with $s(g, x) \leq n - h(n)$ and substituting $s(g, x) = n - s(f, x)$ we get $s(f, x) \geq h(n)$, which contradicts our premise.
We assume $2'$ and that $s(g, x) > n - h(n)$ holds for all x. According to our preceding argumentation, this implies $s(f, x) < h(n)$ so because of $2'$, $deg(f) < n$ which means that $\tilde{f}(\{1, ..., n\}) = \tilde{g}(\emptyset) = \mathbf{E}(g) = 0$, which contradicts our premise. This concludes our proof. □

3 Main Theorem

Theorem 7. *For $n \in \mathbb{N}$ let H be an arbitrary $2^{n-1}+1$ vertex-induced subgraph of Q_n, then $\triangle(H) \geq \sqrt{n}$. Moreover, this inequality is tight if n is a perfect square.*

Proof. The authors of [2] have shown that if n is a perfect square, there exists an induced subgraph H of Q_n such that $\triangle(H) < \sqrt{n}+1$. It follows, that the inequality is tight if $\sqrt{n} \in \mathbb{N}$.

We define $A_n \in \{-1,0,1\}^{2^n \times 2^n}$ as follows:

$$A_1 := \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad A_n := \begin{pmatrix} A_{n-1} & I_{n-1} \\ I_{n-1} & -A_{n-1} \end{pmatrix}$$

Since A_n is symmetric there exist exactly 2^n eigenvalues $\lambda_1 \geq \lambda_2 \geq ... \geq \lambda_{2^n}$. By induction it is easy to see, that

$$A_1^2 = I_2 \qquad A_n^2 = \begin{pmatrix} A_{n-1}^2 + I_{n-1} & 0_{n-1} \\ 0_{n-1} & A_{n-1}^2 + I_{n-1} \end{pmatrix} = n \cdot I_n$$

Let $v_i \in \mathbb{R}^n$ be an eigenvector of A_n with eigenvalue λ_i. Because $n \cdot v_i = A_n^2 \cdot v_i = A_n \cdot A_n \cdot v_i = \lambda_i^2 \cdot v_i$ we get $\lambda_i = \pm\sqrt{n}$. Since $\sum_{i=1}^{n} \lambda_i = tr(A_n) = 0$ each eigenvalue $\lambda_i \in \{\pm\sqrt{n}\}$ has geometric multiplicity 2^{n-1}.

Lemma 7.1. *Let H be an undirected graph with m vertices and $A \in \{-1,0,1\}^{m \times m}$ its adjacency matrix where $a_{i,j} = 0$ if and only if the nodes i and j are non-adjacent in H, then $\triangle(H) \geq \mid \lambda_1 \mid := \mid \lambda_1(A) \mid$. If n is a perfect square, the inequality is tight.*

Proof. Let v be an eigenvector corresponding to the largest eigenvalue λ_1, then $A \cdot v = \lambda_1 \cdot v$. Without loss of generality, let v_1 be the index of v with largest absolute value. Then $\mid \lambda_1 \cdot v_1 \mid = \mid (A \cdot v)_1 \mid = \mid \sum_{j=1}^{m} a_{1,j} \cdot v \mid \leq \sum_{j=1}^{m} \mid a_{1,j} \mid \cdot \mid v_1 \mid \leq \triangle(H) \cdot \mid v_1 \mid$. Conclusively, $\mid \lambda_1 \cdot v_1 \mid = \mid \lambda_1 \mid \cdot \mid v_1 \mid \leq \triangle(H) \cdot \mid v_i \mid$. □

Let $A_n \in \{-1,0,1\}^{2^n \times 2^n}$ be as defined above. A_n corresponds to the adjacency matrix of Q_n if we flip all entries $a_{i,j} = -1$ to $a_{i,j} = 1$ for $i,j \in \{1,...,2^{n-1}\}$. A vertex-induced subgraph H of Q_n is obtained by considering a subset $H \subset V(Q_n) = \{1,...,2^n\}$ of nodes of Q_n. This procedure is equivalent to removing row i and column i corresponding to every node that is not within U from the adjacency matrix A_n. Hence, each vertex-induced subgraph H of Q_n induces its corresponding adjacency matrix A_H of A_n which is a principal submatrix by construction. Therefore, H and A_H satisfy the conditions of Lemma 6.1. This gives us $\triangle(H) \geq \lambda_1(A_H)$. □

It is interesting to note the implications that Lemma 6.1 gives. For instance, given any k-vertex induced subgraph H of Q_n. The adjacency matrix A_H to H as constructed in our proof is symmetric as we have argued before. So there exist exactly k linearly independent eigenvectors $\{v_1, ..., v_k\}$ to eigenvalues $\{\lambda_1, ..., \lambda_k\}$. Then our lemma forces that $\triangle(H) \geq \mid \lambda_1 \mid$. We can further build upon Lemma 6.1.

Lemma 7.2. *Let H be an undirected graph with m vertices and $A \in \{-1, 0, 1\}^{m \times m}$ its adjacency matrix where $a_{i,j} = 0$ if and only if the nodes i and j are non-adjacent in H, then $\triangle(H) \geq \mid \lambda_m \mid := \mid \lambda_m(A) \mid$.*

Proof. We argue analogously, let v be an eigenvector corresponding to the lowest eigenvalue λ_m, then $A \cdot v = \lambda_m \cdot v$. Without loss of generality, let v_1 be the index of v with largest absolute value. Then $|\lambda_m \cdot v_1| = |(A \cdot v)_1| = |\sum_{j=1}^{m} a_{1,j} \cdot v| \leq \sum_{j=1}^{m} |a_{1,j}| \cdot |v_1| \leq \triangle(H) \cdot |v_1|$. □

Combining these two lemmas, we can postulate the following corollary.

Corollary 7.1. *Let $G = (V, E)$ be an undirected graph with m vertices and $A_G \in \{-1, 0, 1\}^{m \times m}$ its adjacency matrix where $a_{i,j} = 0$ if and only if the nodes i and j are non-adjacent in $G = (V, E)$. Since G is undirected, A_G is symmetric and therefore there exist exactly m eigenvalues $\lambda_1 \geq ... \geq \lambda_m$, the eigenvalues of A_G. The following relationship holds, $\triangle(H) \geq \mid \lambda_i \mid$ for $i \in \{1, ..., m\}$.*

This forces for instance, that the adjacency matrix of the 2^{n-1} vertex induced subgraph consisting of all nodes that have an *even number* of 1 entries in their algebraic notation, is the *zero matrix* because every node has degree zero and $\triangle(H) \geq \mid \lambda_i \mid$ for $i \in \{1, ..., m\}$. Moreover, since the adjacency matrix A_G is symmetric, Cauchys Interlace Theorem [5] holds, so for any principal submatrix B of A_G with k rows and columns and eigenvalues $\mu_1 \geq ... \geq \mu_k$, $\lambda_i \geq \mu_i \geq \lambda_{m-k+i}$ for $1 \leq i \leq k$. As any vertex-induced subgraph of G corresponds to a principal submatrix of A_G, we can also formulate the following relationship.

Corollary 7.2. *For all vertex-induced subgraphs $H = (V(H), E(H))$ of $G = (V, E)$ with $\mid V(H) \mid = k$ and $1 \leq i \leq k$ we have $\triangle(H) \geq \mid \mu_i \mid \geq \mid \lambda_{m-k+i} \mid$.*

If we consider any vertex-induced subgraph H of Q_n with $\mid V(H) \mid > 2^{n-1}$, then according to our Corollary 6.2, $deg(H) = \triangle(H) \geq \sqrt{n}$. In other words, maximum degree of a node in H is greater or equal to $\sqrt{n}$. We will use this observation later on.

3.1 Alternative approaches to derive the main theorem

Recently, [9] showed an alternative approach to prove the main theorem of Hao Huang's proof. The alternative approach does not make use of matrices, it solely relies on the construction of a vector space and an edge signing of Q_n. Given a hypercube Q_n, let σ be an edge signing of $+1$ or -1 to the edges of Q_n such that each 4-cycle has an odd number of negative edges. As we shall see, this is the only property that is needed to derive the degree lower bound as Huang did. We extend σ by setting it to 0 for all non-adjacent pairs of vertices in the hypercube. For all vertices $x \in Q_n$, we define the vectors $x^+ \in \mathbb{R}^{2^n}$ and $x^- \in \mathbb{R}^{2^n}$ as follows: for all $y \in Q_n$

$$x^+_{(y)} = \begin{cases} \sqrt{n}, & y = x \\ \sigma(x,y) \end{cases} \qquad x^-_{(y)} = \begin{cases} -\sqrt{n}, & y = x \\ \sigma(x,y) \end{cases}$$

Each of the vectors $x^+_{(y)}$ or $x^-_{(y)}$ entries is non-zero if and only if y and x are adjacent in Q_n or if $x = y$. We use V^+ and V^- to denote the vector subspaces $V^+ = \langle x^+_1, ..., x^+_{2^n} \rangle$ and $V^- = \langle x^-_1, ..., x^-_{2^n} \rangle$. Now, we show the following Lemma.

Lemma 7.3. *If $\{x^+_1, x^+_2, ..., x^+_k\}$ have a linear dependency, then the subgraph induced on the corresponding vertices $\{x_1, x_2, ..., x_k\}$ of Q_n has a vertex of degree at least $\sqrt{n}$.*

Let $\sum a_i \cdot x^+_i = 0$ and $a_i \neq 0$ for at least one $i \in \{1, ..., k\}$. Let $\mid a_j \mid$ be the largest out of all a_i. The vector x^+_j corresponding to a_j has an entry with value $\sqrt{n}$. Since every other vector can contribute at most $\mid a_j \mid$ to this entry there must be at least $\sqrt{n}$ other vectors with value 1 in $\{x^+_1, x^+_2, ..., x^+_k\}$. Because of the construction of x^+_i, these vectors are adjacent to a^+_j. So there exist at least $\sqrt{n}$ neighbours of x^+_j.
We will now show that the dimension of V^+ and V^- respectively is 2^{n-1}. Given any independent set $I = \{x_1, ..., x_k\}$ of Q_n, the vectors $\{x^+_{x_1}, ..., x^+_{x_k}\}$ are linearly independent. Given any $x^+_{x_j}$, since I is an independent set, no two vectors are adjacent. This means that $x^+_{x_j}$ is the only vector that is non-zero at index x_j. This means that the dimension of V^+ and V^- is at least 2^{n-1}.

Lemma 7.4. *The vector spaces V^+ and V^- are orthogonal to each other.*

Proof. Let $x, y \in Q_n$ be arbitrary vectors. Consider x^+ and y^-, we show that $\langle x^+, y^- \rangle = 0$. If $x = y$ then $\langle x^+, y^- \rangle = -\sqrt{n} \cdot \sqrt{n} + \sum_{x:x \sim y} (\sigma(x,y))^2 = -n + n = 0$ If x and y are adjacent they do not share any common neighbour since that would imply an odd cycle of length three. But we have shown that Q_n only has even cycles. The fact that x and y do not share a common neighbour implies that $\langle x^+, y^- \rangle = 0$. If x and y differ in exactly two coordinates, this means that they share exactly two common neighbours u and v. The vertices x, y, u, v form a $4-$cycle and because our edge signing guarantees that the number of negative edges in any $4-$cycle is odd, the equation
$\sigma(x,v) \cdot \sigma(v,y) = -\sigma(x,u) \cdot \sigma(y,u)$ holds. Therefore $\langle x^+, y^- \rangle = \sigma(x,v) \cdot \sigma(v,y) + (x,u) \cdot \sigma(y,u) = 0$. If x and y differ in three or more coordinates there are no common neighbours and $\langle x^+, y^- \rangle = 0$. In total, V^+ and V^- are orthogonal to one another. They

are also both vector subspaces of a vector space of dimension 2^n. We have already shown that the subspaces V^+ and V^- are each of dimension 2^{n-1} or more. Now assume $v \in V^+ \cap V^-$, $\langle v, v\rangle = 0$ because V^+ and V^- are orthogonal and $\langle v, v\rangle = 0 \Leftrightarrow v = 0$ so $v = 0$. This means that $V^+ \cap V^- \subset \{0\}$ so each vectorspace V^+ and V^- is of dimension 2^{n-1}. Now, consider any set of vertices $S = \{x_1, ..., x_k\}$ with $\mid S \mid \geq 2^{n-1} + 1$. The corresponding vectors $x^+_{x_1}, ..., x^+_{x_k}$ or $x^-_{x_1}, ..., x^-_{x_k}$ are linearly dependent and because of our Lemma 7.1, at least one of the vertices has at least $\sqrt{n}$ neighbours. □

On another note, the main theorem has implications for the Turán density of the hypercube Q_n. The Turán density is defined as follows: Let $H \subset Q_n$ be a subgraph or F be a family of such subgraphs. In other words a set of graphs that all share a certain property. A vertex-induced graph $G \in Q_n$ is said to be *free of* H if H is not found to be a subgraph within G. G is said to be *F-free* if no graph $H \in F$ is found to be a subgraph of G. The Turán density on Q_n is now defined as follows. Given a graph $H \subset Q_n$ or a family F of graphs on Q_n, what is the maximum number of edges a vertex induced subgraph $G \subset Q_n$ can have, such that G is free of H or F. If we choose F to be the family of graphs that have maximum degree of at least $\sqrt{n}$ then the main theorem states that the Turán density is exactly 2^{n-1}.

4 Proof of the Sensitivity Conjecture

Proof. Let $H_n = (V, E)$ denote a subgraph of Q_n with $\mid V \mid = 2^{n-1} + 1$, we remember the Theorem of [6].

Theorem (Gotsman and Linial)**.** *The following are equivalent for a monotone function* $h : \mathbb{N} \longrightarrow \mathbb{R}$*:*
(*a*) *For any induced subgraph* H *of* Q_n *with* $|V(H)| \neq 2^{n-1}$*, we have* $\max\{V(H), Q_n \setminus V(H)\} \geq h(n)$.
(*b*) *For any boolean function f, we have* $s(f) \geq h(deg(f))$.

Given the Main Theorem we just proved, we know $\triangle(H) \geq \sqrt{n}$. This satisfies condition (a) of Gotsman and Linial as $\sqrt{\cdot} : \mathbb{N} \to \mathbb{R}$, $n \mapsto \sqrt{n}$ is a monotone function. Now statement (b) holds, so

$$\sqrt{deg(f)} = h(deg(f)) \leq s(f) \tag{4.1}$$

Moreover,

$$bs(f) \leq deg(f)^2 \tag{4.2}$$

according to [3]. Substituting $[\sqrt{deg(f)} \leq s(f)]^4$ into 4.2 gives

$$s(f)^4 \geq deg(f)^2 \geq bs(f) \tag{4.3}$$

□

As mentioned in the preliminary introduction of Q_n and some of its properties important for this thesis, we can use the above theorem as a tool in order to prove, that the maximum independent set of Q_n is 2^{n-1}. Clearly, the set of vertices that have by algebraic notion an even number of 1, is a set of 2^{n-1} vertices and no two vertices are adjacent as they each differ in at least two coordinates. If we however add one more vertex and inspect the hereby vertex-induced subgraph of Q_n, the structure of this graph is also represented by a principal submatrix $B \in \mathbb{R}^{2^{n-2}+1 \times 2^{n-1}+1}$ of A_n, as we just argued in the proof of the Sensitivity Conjecture. Now, B is symmteric so it has exactly $2^{n-1} + 1$ eigenvalues $\mu_1, ..., \mu_{2^{n-1}+1} \in \mathbb{R}$ and since Cauchys Interlace Theorem holds, for all $1 \leq i \leq 2^{n-1} + 1$, $\lambda_i \geq \mu_i \geq \lambda_{2^n - 2^{n-1}+1+i}$ where λ_i denotes the eigenvalues of A_n. Then it must hold that $-\sqrt{n} = \lambda_{2^{n-1}+1} \leq \mu_{2^{n-1}+1} \leq \lambda_{2^{n-1}+2} = -\sqrt{n}$ and since $\triangle(B) \geq \mid \mu_1 \mid = \sqrt{n}$ the subgraph corresponding to B cannot possibly be an independent set. By means of the same line of argument there cannot exist a vertex-induced subgraph with more than $2^{n-1} + 1$ vertices where no two nodes are connected, since any $2^{n-1} + 1$ vertex-induced subgraph would already have a node with degree greater or equal to $\sqrt{n}$. Conclusively, we prove the claim that the size of a maximum independent set of Q_n is 2^{n-1}.

4.1 Further thoughts

By virtue of Huang's proof, the bound for block sensitivity is quartic, $bs(f) \leq s(f)^4$, but the existing exemplary boolean functions yield at most a quadratic separation between sensitivity and block sensitivity. One example is the following function f composed of a logical disjunction of boolean functions g. It is borrowed from [12]. For $n \in \mathbb{N}$ consider $g : \{0,1\}^{2n} \to \{0,1\}$ $g(x) = 1$ if and only if x has value 1 on exactly two succeeding variables where the first one has an odd index. For instance, $g((1,1,0,...,0)) = 1$ whereas $g((0,1,1,0,...,0)) = 0$. In any other case $g(x) = 0$. Considering $x = (1,1,0,...,0)$, a flip of any index i will force $g(x) \neq g(x^i)$, so $s(g) = 2n$. We define $f : \{0,1\}^{4n^2} \to \{0,1\}$, $f(x_{1,1}, x_{1,2}, ..., x_{2n,2n}) = \bigvee_{i=1}^{2n} g(x_{i,1}, ..., x_{i,2n})$. The sensitivity of f is equal to that of g, $s(f) = 2n$. For the block sensitivity of f, we get $bs(f) = 2n^2$ when we choose $v = (0,...,0) = (x_{1,1}, ..., x_{2n,2n}$ as input vector since flipping two succeeding indices starting at index 1 changes the value of the respective function $g(x_{i,1}, ..., x_{i,2n}$ from 0 to 1. This can be done for exactly n distinct pairs of indices $j, j+1$ for an uneven integer j. Since there are $2n$ distinct functions g this gives a total of $2n \cdot n$ pairwise disjoint indices which when flipped change the output value of f from 0 to 1. This means $bs(f) \geq \frac{1}{2}s(f)^2$. There are functions building upon this construction with greater gap between $bs(f)$ and $s(f)$ [13]. Nonetheless, all known constructions have an at most quadratic separation. There exist further measurements of complexity that we may try to use in order to narrow down the true polynomial bound between $bs(f)$ and $s(f)$. A promising measurement is the so called certificate complexity. The certificate complexity describes how many bits of the input must be revealed to you (by someone who knows all the input bits) in order to convince you of the value of the function. In less prosaic terms, a 1-certificate (0- certificate) for a boolean function f is an assignment to some subset of the variables that forces the value of f to 1(0). The certificate complexity of f on an input x , $C_x(f)$, is the size of the smallest certificate that agrees with x. The certificate complexity of f , $C(f)$, is the maximum over all x of $C_x(f)$. For certificate complexity and block sensitivity, we can establish the following relationships.

Lemma 7.5. *$s(f) \leq bs(f) \leq C(f)$ and $bs(f) \geq \sqrt{C(f)}$*

Proof. The inequality $bs(f) \leq C(f)$ follows from the fact that for any input x, any certificate for x must include at least one variable from each set f is sensitive to on x. As for $bs(f) \geq \sqrt{C(f)}$, let x be an input that achieves certificate complexity on f, in other words $C(f,x) = C(f)$. We pick a minimal subset S_1 of indices such that $f(x^{S_1}) \neq f(x)$, then another minimal set S_2 disjoint from S_1 with $f(x^{S_2}) \neq f(x)$. This procedure obviously terminates, so we continue this process until we do not find any more minimal subsets. Now, all subsets $\{S_1, ..., S_j\}$ are mutually disjoint and $\bigcup_{i=1}^{j} S_i$ is a certificate of x on f, otherwise we would find another minimal set disjoint to the other sets that changes the value of $f(x)$ when its indices are flipped in x. $\sum_{i=1}^{j} \mid S_i \mid \geq C(f,x) = C(f)$. The two inequalities hold,

$$bs(f,x) \geq j \tag{4.4}$$

because f is sensitive to each block S_i on x. Also,

$$bs(f, x^{S_i}) \geq \mid S_i \mid \; i \in \{1, ..., j\} \tag{4.5}$$

because every S_i is minimal. So f must be sensitive on x^{S_i} on any index from S_i. Now, if $j \geq \sqrt{C(f)}$ then with (4.4) we get $bs(f) \geq \sqrt{C(f)}$. Otherwise, if $j < \sqrt{C(f)}$ at least one S_i has to have a larger size than $C(f)$ so with (4.5) we get $bs(f, x^{S_i}) \geq \mid S_i \mid > \sqrt{C(f)}$. □

The inequality $bs(f) < C(f)$ is strict if we consider the function $f(x) = 1$ if and only if x has 1 at exactly $\frac{n}{2}$ indices, for the sake of simplicity we assume that $4 \mid n$. Then $bs(f) = \frac{3n}{4}$ and $C(f) = n$.

Another way of looking at the relationship between sensitivity and block sensitivity is the following. Given a boolean function $f : \{0,1\}^n \to \{0,1\}$, we construct a two-colouring in Q_n. Without loss of generality, every node x with $f(x) = 1$ is coloured red, if $f(x) = 0$ it is coloured green. Now, for any input x, $s(f, x)$ is the number of adjacent nodes in opposite colour. Analogously, $bs(f, x)$ is the maximum number of node disjoint paths from x to a set of nodes all of which are of opposite colour and more importantly, each direction can be chosen at most once. A path is to be understood as a sequence of edges from G_n. We denote a direction as $v \in \{0,1\}^n$ with exactly one variable set to 1 and the others set to 0. Given this approach, the block sensitivity is bounded by $bs(f) \leq s(f) + \lfloor \frac{n - s(f)}{2} \rfloor$.

Certificate complexity on our two-coloured Q_n model is the minimal number of nodes v that suffice to cover exactly either the red or green nodes. Two vectors $(0, ..., 0), (1, 0, ..., 0)$ can be condensed to $(\_, 0, ..., 0)$ as we have done before. Then, certificate complexity is n minus the dimension of the largest monochromatic hypercube in Q_n. Yet another perspective onto sensitivity, block sensitivity and certificate complexity is that of Quine McCluskey tables. A Quine McCluskey table is a graphic representation of a boolean function and its values, as can be seen in the figure below for a boolean function with four-dimensional input.

Here, the index in the bottom left of each square corresponds to the binary input vector that evaluates to the index. The index of the top lefthand square is 0 for instance which means $f(0, 0, 0, 0) = 1$. The index of the bottom-right square is 12 which means $f(1, 1, 0, 0) = 1$. Now, the sensitivity of f on an input x is the number of squares of opposite value that can be reached by moving along one direction on the McCluskey table. The block sensitivity of f on x is the number of paths to squares of opposing value where each direction can only be taken at most once. The certificate complexity of f on an input x is n minus the highest dimensional subcube that encompasses x as can be seen in the figure above. A subcube of dimension two is created by merging two adjacent fields which differ in exactly one coordinate value. This can also be denoted algebraically by combining two vectors for instance $(0, 0, 0, 1)$ and $(1, 0, 0, 1)$ into $(\_, 0, 0, 1)$ where the underscore denotes an arbitrary value. Each subcube has a dimension of a power of two. Thus, a subcube of dimension four is created as can be seen in the figure by combining two subcubes of dimension two which differ in exactly one coordinate. The

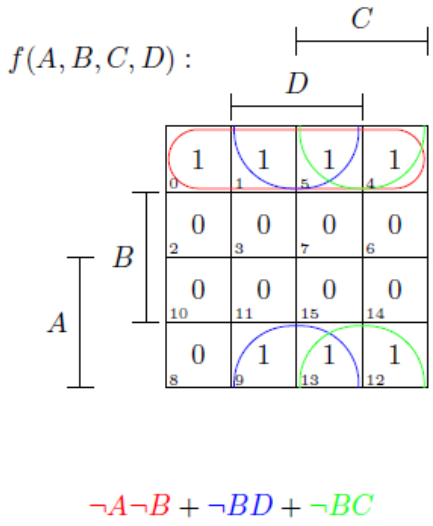


Figure 6: A McCluskey table

cubes $(\_, 0, 0, 1)$ and $(\_, 0, 0, 0)$ for instance are merged into the cube $(\_, 0, 0, \_)$. On a side note, this procedure can be linked to the inductive algebraic construction of the hypercube Q_n which we will use in chapter five.

The main theorem has implications in group theory. With its help, the following theorem [1] was proven. To understand it, we introduce the concept of Cayley graphs and generating sets of a group.

Let G be a group, a generating set $S \subset G$ with regard to G is a set of elements such that every $g \in G$ can be written as a combination (under the group operation) of finitely many elements $s_1, ..., s_n \in S$ of the subset S and their inverses. The identity element e_G is not part of S. A Cayley graph $\Gamma(G, S)$ is a colored, directed graph, constructed from a group G and a generating set $S \subset G$ as follows:

Every $g \in G$ represents a vertex in $\Gamma(G, S)$. Any $s \in S$ that is assigned a color c_s. For any $g \in G$ and $s \in S$ the vertices corresponding to the elements g and gs are joined by a directed edge of colour c_s. Thus the edge set $E(\Gamma)$ consists of pairs of the form $(g, g \cdot s)$ with $s \in S$ providing the color. The figure below exemplarily depicts a Cayley graph.

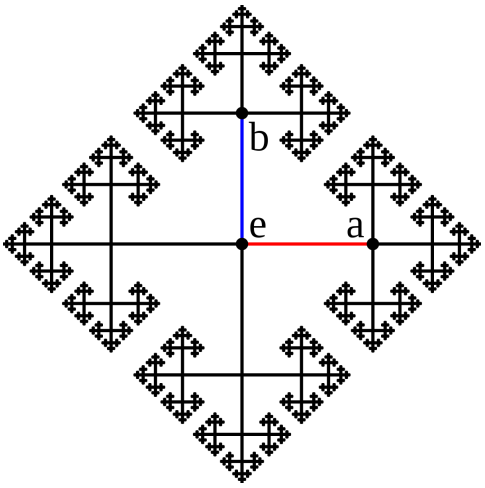


Figure 7: A Cayley graph

Cayley graphs are always vertex-transitive and regular. A graph G is vertex-transitive, if for every $v_1, v_2 \in G$ there exists an automorphism $f : V(G) \to V(G)$ with $f(v_1) = v_2$. For any $g \in G$ $\Phi_g : G \to G$ is an automorphism. This is because if $\Phi_g(s_1) = \Phi_g(s_2)$ then $g \cdot s_1 = g \cdot s_2$ then $g^{-1} \cdot g \cdot s_1 = g^{-1} \cdot g \cdot s_2$ so $s_1 = s_2$ and thus Φ_g is an injective mapping. Since any injective endomorphism must also be surjective, Φ_g is an automorphism. Now suppose $v_1, v_2 \in G$. We pick $g = v_2 \cdot v_1^{-1}$ then $\Phi_g(v_1) = v_2 \cdot v_1^{-1} \cdot v_1$ which completes the proof of vertex-transitivity. This also means that the automorphism group operates transitively on G. The automorphism group of G is the set of all automorphisms $\Phi : G \to G$ with the function composition as inner binary operation. It is said to act from the left on G if the following two statements hold $e_{Aut(G)} \circ g = g$ for all $g \in G$ and $\Phi_1(\Phi_2 \cdot g) = (\Phi_1 \circ \Phi_2) \cdot g$ for all $\Phi_1, \Phi_2 \in Aut(G)$ and $g \in G$. To see this, assume G is a vertex-transitive graph. It is said to act transitively from the left if for a fixed $g \in G$ then for any $h \in G$ there exists $\Phi \in Aut(G)$ such that $\Phi(g) = h$. This is a weakened demand of vertex-transitivity.

Cayley graphs are also regular since every vertex-transitive graph G is regular. Because for arbitrary $v_1, v_2 \in G$ we find a graph automorphism $\Phi : G \to G$ with $\Phi(v_1) = v_2$. Because $u, v \in G$ are adjacent if and only if $\Phi(u), \Phi(v)$ are adjacent, any automorphism maps the neighbours of v_1 bijectively onto the neighbours of v_2. Since this holds for any v_1, v_2, every node must have the same number of adjacent nodes which is the definition of regularity. The hypercube Q_n can be interpreted as the Cayley graph of the group $G = \mathbb{Z}_2^n$ where the generating set is the set of all $g \in G$ that have exactly one coordinate with value 1 and the rest of which have value 0. Since G is an abelian group, for every $(g, s \cdot g)$ we have $(s \cdot g, s^{-1} \cdot s \cdot g) = (g \cdot s, g)$ so $\Gamma(G, S)$ can be interpreted as an undirected graph as was done so in the following theorem.

Theorem 8. *For any Cayley graph $G = (\mathbb{Z}_2^n, S)$ of $\mathbb{Z}_2^n$ with respect to any generating set S, and for any subset $U \subset \mathbb{Z}_2^n$ of cardinality $\mid U \mid > 2^{n-1}$, the maximum degree of the induced subgraph H of G on U satisfies $\triangle(H) \geq \sqrt{\mid S \mid}$.*

Proof. The theorem was discovered by the authors of [1]. Let $G = (\mathbb{Z}_2^n, S)$ be a Cayley graph with respect to a generating set $S = \{s_1, ..., s_d\}$. That is every $g \in G$ can be written as a finite composition of elements of S. In other words $s_{i_1} \cdot ... \cdot s_{i_k} = g\}$ for $i_1, ..., i_k \in \{1, ..., d\}$. Additionally, we assume $S = S^{-1}$. First, it is easy to see that for simplicity's sake, G can be viewed to be an undirected graph because if $(g, g \cdot s) \in E(G)$ then $(gs, gs \cdot s^{-1}) \in E(G)$, so $(gs, g) \in E(G)$. Without loss of generality we assume that G is connected. Otherwise, G consists of isomorphic connected components on the cosets of $\langle S \rangle$. Suppose there exist two or more disconnected components in G. This means there must be $g_1, g_2 \in G$ that are not connected. We define an isomorphism $\Phi : G \to G$ by $\Phi(g_1) = g_2$, $\Phi(g_2) = g_1$ and $\Phi(h) = h$ if $h \notin \{g_1, g_2\}$. If $\{g, g \cdot s_i\} \in E(G)$, then $\{\Phi(g), \Phi(g \cdot s_i\} = \{g_2, g_2 \cdot s_i\}$. The reverse is also true, which leaves us with $\{g_1, g_1 \cdot s_i\} \in E(G) \leftrightarrow \{g_2, g_2 \cdot s_i\} \in E(G)$ which proves isomorphic connectedness. Indeed, if G is not connected, any set $U \subset \mathbb{Z}_2^n$ with $\mid U \mid > \frac{G}{2}$ has more than half the vertices of at least one of the isomorphic connected components. Thus one can deduce the result from the connected case. Let Q_d denote the d-dimensional hypercube, which can be interpreted as the Cayley graph of $\mathbb{Z}_2^d$ with respect to the generating set $S = \{e_1, ..., e_d\}$. Let $\Phi : \mathbb{Z}_2^d \to \mathbb{Z}_2^n$ be a linear transformation with $\Phi(e_i) = s_i$. Then Φ is onto since the s_i span $\mathbb{Z}_2^n$. Let $U \subset \mathbb{Z}_2^n$ be a set with more than half the vertices of $\mathbb{Z}_2^n$. Then $V := \Phi^{-1}(U) \subset \mathbb{Z}_2^d$ contains more than half the vertices of $\mathbb{Z}_2^d$. According to the main theorem, there exists a vertex $v \in \mathbb{Z}_2^d$ with distinct adjacent vertices $\{v_1, ..., v_k\}$ where $k \geq \sqrt{d}$. Therefore, the vertex $\Phi(v) \in U$ is adjacent to the distinct vertices $\{\Phi(v_1), ..., \Phi(v_k)\}$. To see this, we first note that if $\{v_i, v_j\}$ are adjacent in $\mathbb{Z}_2^d$ then $v_i - v_j = v_i + v_j \in \{e_1, ..., e_d\}$. Then, $\Phi(v_i - v_j) = \Phi(v_i + v_j) \in \{s_1, ..., s_d\}$ which means that $\Phi(v_i) \neq \Phi(v_j)$. □

In fact there was a recent advancement by the authors of [11] who generalized the preceding conjecture.

Theorem 9. *For any Cayley graph G such that G is abelian and any $U \subset G$ of size $\mid U \mid \geq \frac{|G|}{2}$ the induced subgraph H_U of G on U has maximum degree at least $\sqrt{\frac{(|S|+t)}{2}}$ where t is the number of elements in S of order 2.*

Proof. First, we use the main theorem to establish a corollary:

Corollary 9.1. *Let $G = \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_d}$, $S = \{\pm e_1, ..., \pm e_d\}$ and $X = \Gamma(G, S)$ the Cayley graph of G with respect to S. For any $U \subset G$ satisfying $\mid U \mid > \frac{|G|}{2}$ there exists an element $u \in U$ and $k \geq \sqrt{d}$ distinct indices $i_1, ..., i_k \in \{1, ..., d\}$ such that for $j \in \{1, .., k\}$ $u + e_{i_j} \in U$ or $e - e_{i_j} \in U$.*

To see this, we define $U_r := \{r + \sum_{i \in T} e_i : T \subset \{1, ..., d\}\}$ and observe that $\mathbf{E}_r(\mid U_r \cap U \mid) > 2^{n-1}$. In other words, the expected value over a uniform random distribution of r is more than 2^{n-1}. There must exist $g \in G$ with $\mid U_g \cap U \mid > 2^{n-1}$. The induced subgraph of U_g, namely $X(U_g)$ is isomorphic to Q_d and because $\mid U_g \cap U \mid > 2^{n-1}$

$deg(X(U_g \cap U)) \geq \sqrt{d}$ holds. This proves the corollary.
Now onto the proof of Theorem 8, let $G = \mathbb{Z}_{m_1} \times ... \times \mathbb{Z}_{m_k}$,
$S = \{s_1, ..., s_t, s_{t+1}, ..., s_d, -s_{t+1}, ..., -s_d\}$ and m be the least common multiple of $\{m_1, ..., m_k\}$. In other words $m := lcm(m_1, ..., m_k)$. Let $X' = \Gamma(\mathbb{Z}_m^d, T)$ be the Cayley graph of $\mathbb{Z}_m^d$ with respect to the generating set $T := \{\pm e_1, ..., \pm e_d\}$. Just as with the proof of Theorem 7, we define $\Phi : \mathbb{Z}_m^d \to G$ to be a linear map defined by $\Phi(e_i) = s_i$. Since S is a generating set, the linear map Φ is onto. The inverse image of each $g \in G$, namely $\Phi^{-1}(g)$ contains $\mid ker(\Phi) \mid$ elements and with the fundamental homomorphism theorem $\frac{|H|}{|ker(\Phi)|} \cong \mid image(\Phi) \mid$ for any group homomorphism $\Phi : H \to G$ we can postulate the equation $\frac{|H|}{|G|} = \mid ker(\Phi) \mid$. It follows that $\mid \Phi^{-1}(g) \mid = \frac{m^d}{|G|}$ so $\Phi^{-1}(U) = \frac{m^d}{|G|} \cdot \mid U \mid > \frac{m^d}{|G|} \cdot \frac{|G|}{2}$. Due to our Corollary 8.1 there is a vertex $h \in \Phi^{-1}(U)$ and $k \geq \sqrt{d}$ distinct indices $i_1, ..., i_k \in \{1, ..., d\}$ such that for all $j \in \{1, .., k\}$ either $h + e_{i_j} \in \Phi^{-1}(U)$ or $h - e_{i_j} \in \Phi^{-1}(U)$. Now we consider $h_j \in \{h \pm e_{i_j}\}$ such that $h_j \in U$ and see that for $j' \neq j \in \{1, ..., k\}$ $\Phi(h_{j'}) - \Phi(h_j) = \Phi(h) \pm \Phi(e_{i_{j'}}) - \Phi(h) \mp \Phi(e_{i_j}) = \pm s_{i_{j'}}, \mp e_{i_j} \neq 0$. The argument is analogous to the one from Theorem 7, all $\Phi(h_1), ..., \Phi(h_k)$ are distinct, lie within U and are adjacent to $\Phi(h) \in U$ in $X(U)$ with $X = \Gamma(G, S)$. Because $\mid S \mid = t + 2 \cdot (d - t)$, $d = \frac{|S|+t}{2}$ as we claimed.

□

5 Further structural restrictions

5.1 $K_{1,a}$ subgraphs

In graph theory, a *k-colouring* of a graph $G = (V, E)$ is a special case of graph labeling; it is an assignment from a set of k distinct labels, traditionally called "colors", to elements of a graph subject to certain constraints. In its simplest form, it is a way of coloring the vertices of a graph such that no two adjacent vertices are of the same color; this is called a proper vertex coloring. A *non-balanced two colouring* of a graph is a proper two-colouring where the number of nodes assigned with one colour is different from that of the number of nodes assigned with the other colour. In the following, we will only use unbalanced two-colourings of the Q_n. Let $n \in \mathbb{N}$. For a non-balanced two-colouring of Q_n consider the node set of the majority colour and the subgraph of Q_n that this set induces. We will refer to the subgraph as H in the following and whenever we speak of an induced subgraph we will implicitly assume that it is a subgraph induced by the majority colour of an unbalanced two-colouring.
Using Corollary 6.2 and our postceding observation, we know that for any vertex induced subgraph H with more than 2^{n-1} nodes $\triangle(H) \geq \sqrt{n}$ holds. In other words, given any H with more than 2^{n-1} nodes, the graph has at least one node with at least $\sqrt{n}$ neighbours in it. Adding onto Huangs findings and our previous observations it is of interest to examine if there are further properties of the subgraph induced by the node of maximum degree and its neighbours. Consider for instance the graph $K_{1,a}$ that we introduced in the beginning of this chapter, where $a \leq n$, $a \in \mathbb{N}$. A question that springs to mind is if this graph can be found in any or perhaps even all majority colour induced subgraphs of Q_n. Or more formally put, does there exist a non-balanced 2-colouring such that the majority colour induces a subgraph with a $K_{1,a}$ structure for every $\sqrt{n} \leq a \leq n$ or even $1 \leq a \leq n$? If so, does this even hold for every majority colour induced subgraph?
It is easy to see that not every subgraph has a $K_{1,a}$ graph for any $1 \leq a \leq n$. In order to validify our claim we inspect the graph Q_n itself. It is induced by the majority colouring if every node is coloured with one colour. Recall, that we have proven that there exists a hamiltonian cycle in Q_n. Therefore there cannot exist a $K_{1,a}$ graph in Q_n. Now the question whether $K_{1,a}$ even exists in any subgraph remains to be examined. We postulate and prove the following observation.

Theorem 10. *Given Q_n and $n \geq 4$. For each $a \in \{1, ..., n\}$ there exists a subgraph $G_n = (V_n, E_n)$ with $\mid V_n \mid > 2^{n-1}$, so that G_n has exactly two connected components, one of which is $K_{1,a}$ and the other component is not a $K_{1,b}$ graph for $b \in \{1, ..., n\}$.*

Proof. We will use a technique resembling structural induction, which I will first conceptionally outline. We will define a set of subgraphs G_n in Q_n alongside with a set of three properties that will hold for all of our subgraphs. These three properties force the subgraph G_n to satisfy the conditions from our Theorem 6. Then, given Q_{n+1}, we reduce it to Q_n for which know because of our induction hypothesis, that it contains G_n. Then we expand in G_n to a G_{n+1} graph in Q_{n+1} whilst preserving all three properties which in turn force G_{n+1} to comply with all conditions from our Theorem 6. Hopefully clear

by now, this technique yields proof of our claim. In the following, I included figures to exemplarily depict the process of reducing Q_{n+1} to Q_n, isolating and extending G_n to G_{n+1} in Q_{n+1} for a set of different $K_{1,a}$ graphs. Now onto the more detailed proof.
Since any node within Q_n has exactly *degree* n, no node within a subgraph of Q_n can have a degree higher than n, so $a \leq n$ is our premise. In Q_4 for every $a \in \{1, ..., 4\}$ we construct a subgraph G_4 with $\mid V_n \mid \geq 2^3 + 1$ and exactly one $K_{1,a}$ structure. We use the algebraic notation of Q_n referenced in the introduction of the n-hypercube as node coordinates within the succeeding figures. For purposes of brevity and convenience, _ is used to symbol any possible entry for a node of Q_n, hence $\{(\_, 1, 0)\} = \{(0, 1, 0), (1, 1, 0)\}$. In the following figures, there are nodes of red, green and no colour. Red nodes represent the set of nodes forming a $K_{1,a}$ graph and the set union of red nodes and green nodes form a G_n graph. The nodes without colour are not part of the subgraph.
The node set $\{(0,0,0,0), (1,0,0,0), (0,1,1,0), (1,1,1,0)\} \cup$
$(\{(\_, \_, \_, 1)\} \setminus \{(0,0,0,1), (1,0,0,1)\})$ has a $K_{1,1}$ graph formed by the nodes $(0,0,0,0)$ and $(0,1,0,0)$ as depicted in the figure below.

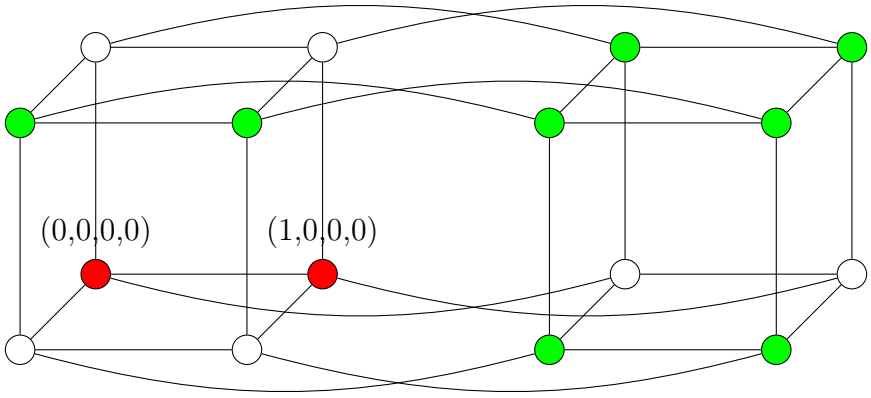


Figure 8: A graph with a $K_{1,1}$ subgraph

The node set $\{(0,0,0,0), (1,0,0,0), (0,1,0,0), (1,1,1,0)\} \cup$
$(\{(\_, \_, \_, 1)\} \setminus \{(0,0,0,1), (1,0,0,1), (0,1,0,1)\})$
has a $K_{1,2}$ structure.

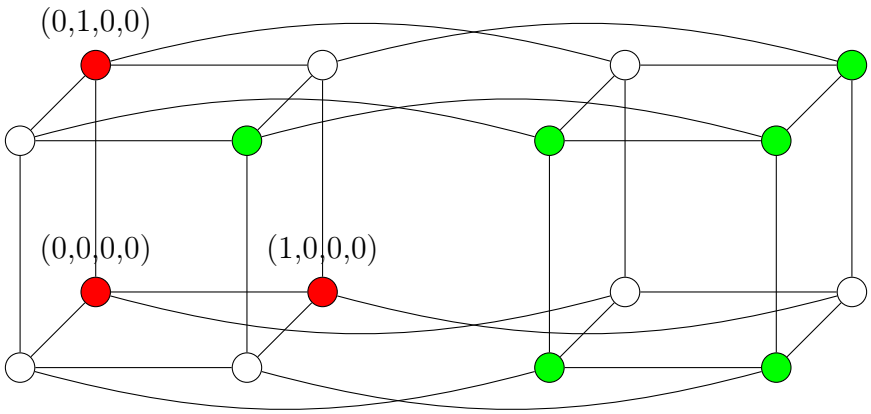


Figure 9: A graph with a $K_{1,2}$ subgraph

The node set $\{(0,0,0,0),(1,0,0,0),(0,1,0,0),(0,0,1,0),(1,1,1,0)\} \cup \{(\_,\_,\_,1)\} \setminus \{(0,0,0,1),(1,0,0,1),(0,1,0,1),(0,0,1,1)\}$ has a $K_{1,3}$ structure.

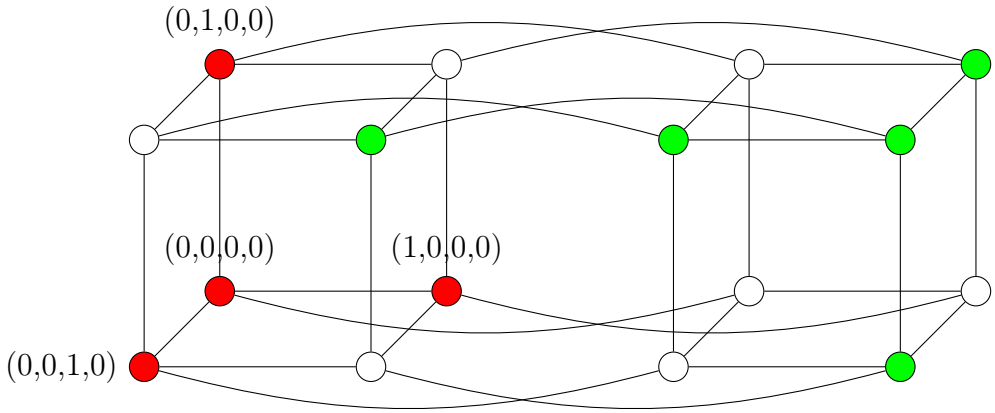


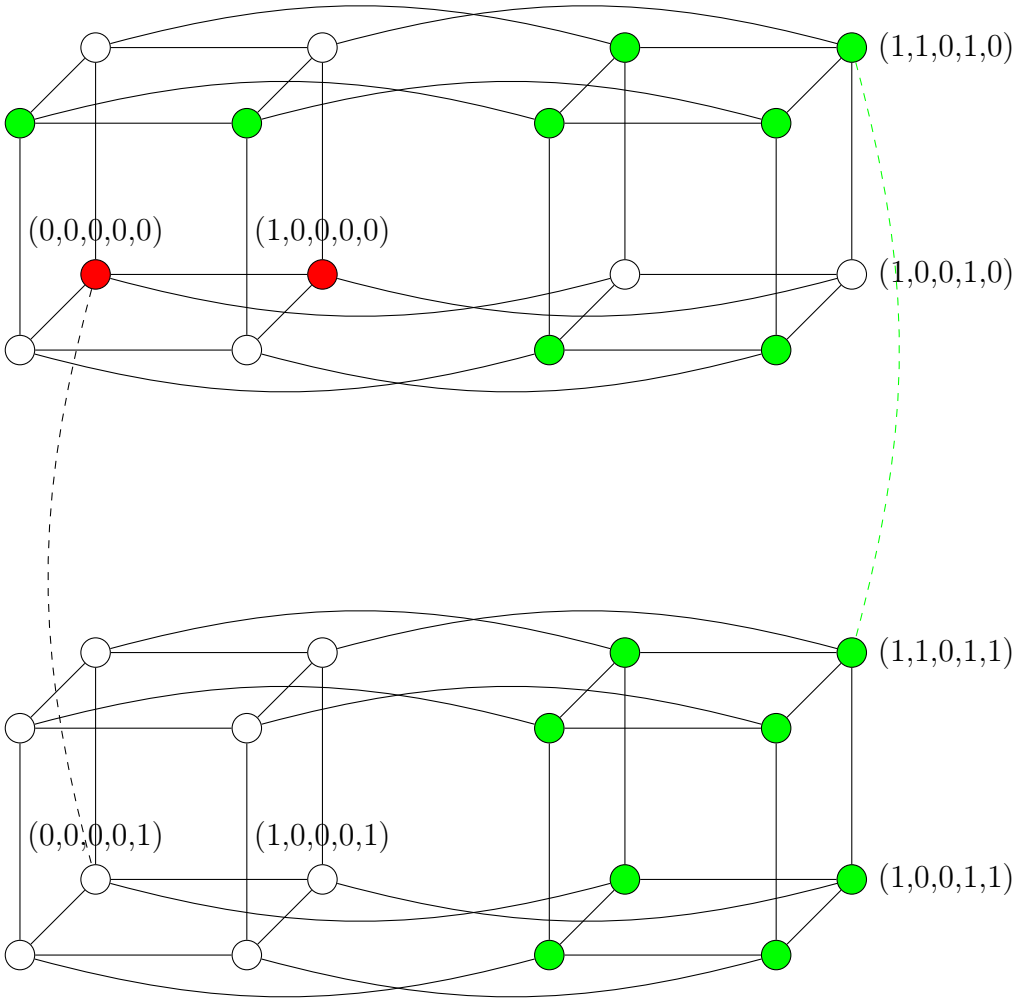
Figure 10: A graph with a $K_{1,3}$ subgraph

Now for $n \geq 4$, we proceed by induction over n. There exists a subgraph $G_n \subset Q_n$ so that the following properties hold:

1. There exists an unbalanced two-colouring with one $K_{1,a}$ graph in G_n.
2. There exist exactly two disjoint components in G_n.
3. $\mid V_n \mid > 2^n$.

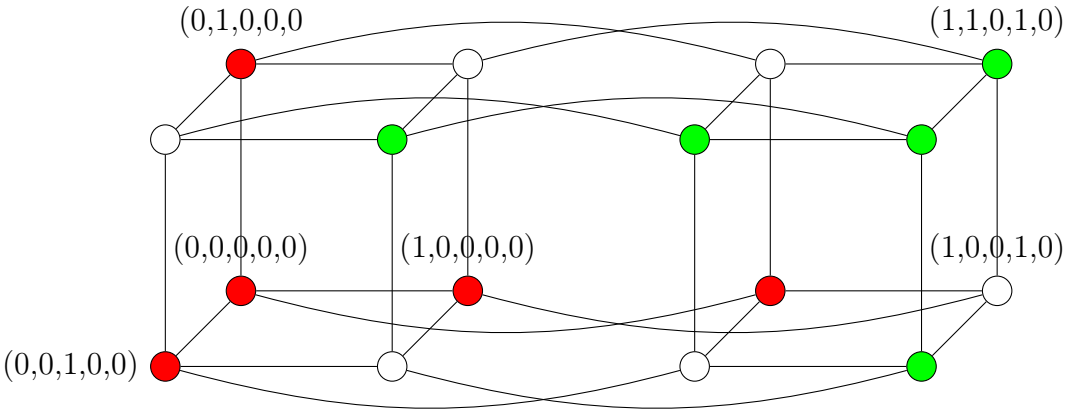
As foretold in the beginning of our proof, given Q_{n+1}, we will reduce it to Q_n for which we know because of our induction hypothesis, that all three properties listed above must hold. Then, we expand the $K_{1,a}$ graph in G_n to either a $K_{1,a}$ or $K_{1,a+1}$ graph in G_{n+1} whilst preserving all three properties. Via structural induction this technique yields proof

of our claim. In the following, we will assume that $1 \leq a \leq n-1$ because we prove our claim for any $K_{1,a}$ graph but $K_{1,n}$. First, we consider the set of nodes that make up G_n, namely V_n. Since Q_{n+1} has one more dimension than Q_n and therefore G_n, we will denote V_n in Q_{n+1} algebraically as $S_{n+1} := \{(v_1, ..., v_n, 0)\}$ for all $(v_1, ..., v_n) \in V_n$. Without loss of generality we denote the node w in $K_{1,a}$ that is connected to every other node in $K_{1,a}$ as $w_{K_{1,a}} = (0, ..., 0)$. More formally, $w_{K_{1,a}} \in K_{1,a}$ and $deg(w_{K_{1,a}}) = a$. All of its adjacent nodes $\{k_1, ..., k_a\}$ we will denote as $k_i = (0, ..., 1, 0, ..., 0)$ with 1 as entry at index i. Now, we will define another set of nodes U_{n+1} in Q_{n+1} and see that the set union of these two sets of nodes, U_{n+1} and S_{n+1} already gives us G_{n+1}. Let $U_{n+1} := \{(\_, ..., \_, 1, 1)\}$. We set $V_{n+1} := S_{n+1} \cup U_{n+1}$, then $\mid V_{n+1} \mid = \mid S_{n+1} \mid + \mid U_{n+1} \mid \geq 2^{n-1} + 1 + 2^{n-1} = 2^n + 1$ because S_{n+1} and U_{n+1} are disjoint and (3) holds for V_{n+1}.

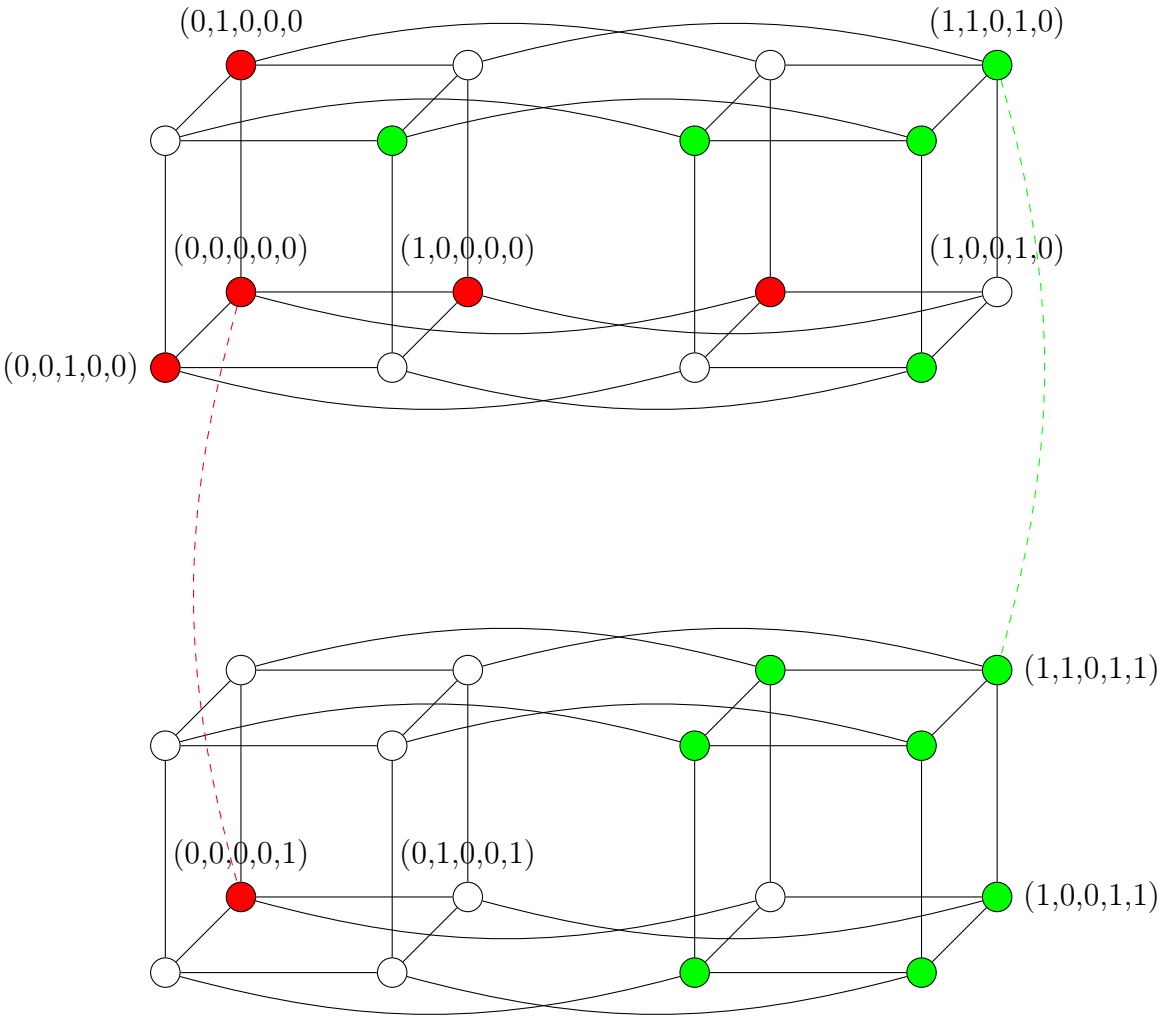


The figure above depicts our technique. We reduced Q_{n+1} to Q_n and extended the $K_{1,a}$ graph in G_n to G_{n+1} in Q_{n+1}. This extension works analogously for each $a \in \{1, ..., n-1\}$. In S_{n+1} there exists at least one node $v = (v_1, ..., 1, 0)$ that is not adjacent to $K_{1,a}$. This can be easily seen because of the algebraic construction of $K_{1,a}$. Because of (2), v must

be connected to the other component of G_{n+1} that is canonically induced by the vertex set of G_n. Because of the construction of U_{n+1}, v is connected to at least one node in U_{n+1}, therefore (2) and (1) hold in V_{n+1} and therefore in G_{n+1}.
As one will have noted, up until now since we assumed $a \in \{1, ..., n-1\}$, our technique covers neither $K_{1,n}$ nor $K_{1,n+1}$ in Q_{n+1}. This is adressed in the subsequent paragraph. Consider the following subgraph G_4 in Q_4,
$\{(0,0,0,0)(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1), (1,1,1,0)\} \cup$
$\{(v_1, v_2, v_3, 1) \mid (v_1, v_2, v_3) \notin K_{1,4}\}$.



It has a $K_{1,4}$ structure and properties $(1) - (3)$ hold. By induction we expand this set of nodes to construct a vertex induced subgraph G_{n+1} of Q_{n+1} that has a $K_{1,n+1}$ or $K_{1,n}$ structure respectively whilst preserving properties $(1) - (3)$. Again, we expand the set of nodes V_n of G_n to $S_{n+1} := \{(v_1, ..., v_n, 0) \mid (v_1, ..., v_n) \in V_n\}$. Let $\tilde{U}_{n+1} := (\{\_, ..., \_, 1, 1)\} \setminus \{(0, ..., 0, 1, 1)\}$ be a set of nodes in Q_{n+1}. Because all but the last two indices of any node in $\tilde{U}$ is fixed, $\mid \tilde{U}_{n+1} \mid = \frac{2^{n+1}}{2^2} - 1 = 2^{n-1} - 1$. By construction, the node $a = (0, ..., 0, 1)$ is not connected to $\tilde{U}_{n+1}$ but expands the $K_{1,n}$ structure to $K_{1,n+1}$. The nodes in $\tilde{U}_{n+1}$ are connected to the nodes in the one of two components in G_{n+1} canonically induced through G_n, that does not have the $K_{1,n}$ structure. This must be true according to (2). We set $U_{n+1} = \tilde{U}_{n+1} \cup \{a\}$ and $V_{n+1} := V_n \cup U_{n+1}$. The number of nodes in V_{n+1} is $\mid V_{n+1} \mid = \mid V_n \mid + \mid U_{n+1} \mid = (2^{n-1} + 2) + 2^{n-1} = 2^n + 2 > 2^n$. The resulting subgraph G_{n+1} has exactly two components, one of which is the $K_{1,n}$ structure, the other component is not a $K_{1,a}$ structure as argued prior. The $K_{1,n}$ structure is expanded to a $K_{1,n+1}$ structure. For the new vertex set V_{n+1}, $(1) - (3)$ hold.



Since (2) holds in G_n, there must be at least one node $a = (a_1, ..., a_{n-1}, 0) \in Q_n$ that is not matched by either component of V_n. If we set $U_{n+1} := \tilde{U}_{n+1} \cup (a, 1)$, it is easy to see that U_{n+1} is connected to the component in G_{n+1} induced through G_n without the $K_{1,n}$ structure so the statements $(1) - (3)$ hold. All whilst the $K_{1,n}$ structure remains unaltered.
Conclusively, for $1 \leq a \leq n$ and $n \geq 4$ we can construct a non-balanced two-colouring of Q_n whose majority colour induces a subgraph with exactly two components and exactly one $K_{1,a}$ structure.

□

6 Conclusions

In this thesis we explored the techniques that Hao Huang used to prove the Sensitivity Conjecture as well as the proof itself. We used these techniques to establish further insight into the relationship between a special category of matrices and the corresponding undirected graphs they induce. Given a matrix with entries in $\{-1, 0, 1\}$ and 0 as entry if and only if there exists no edge between the nodes i and j in the corresponing induced graph, the degree of the graph is at least high as the highest absolute value of any eigenvalue of the matrix. Since these matrices are symmetric they are diagonizeable and have as many eigenvalues as dimensions. We have seen that the same holds for every vertex induced subgraph of the matrix.

We became acquainted with structural features of the n-hypercube which are responsible for yielding a proof of the main theorem that does not make use of the matrix that Huang employed but relies on a special edge signing. Moreover we have looked at an application of Huangs main theorem applied to proofs targeting Cayley graphs of $\mathbb{Z}_2^n$ and more generally abelian Cayley graphs.

The best separation between sensitivity and block sensitivity is $bs(f) = \frac{2}{3}s(f) - \frac{1}{3}s(f)$ whilst Huang has shown a quartic upper bound. It remains to be seen whether the quartic upper bound is tight or whether it can be lowered.

References

[1] N. Alon and K. Zheng. "Unitary signings and induced subgraphs of Cayley graphs of $\mathbb{Z}_2^n$". In: *arXiv:2003.04926* (2020).

[2] F. Chung et al. "On induced subgraphs of the cube". In: *Journal of Combinatorial Theory, Series A* (1988), pp. 180–187.

[3] F. Chung et al. "Properties and applications of boolean function composition". In: *Proceedings of the 4th conference on Innovations in Theoretical Computer Science* (2013), pp. 441–454.

[4] Bruno Escoffier and Vangelis Paschos. "An Alternative proof of SAT NP-Completeness". In: *hal-00017602 pp.10* (2004).

[5] S. Fisk. "A very short proof of Cauchy's interlace theorem for eigenvalues of hermitian matrices". In: *American Mathematical Monthly* (2005), p. 112.

[6] C. Gotsman and N. Linial. "The equivalence of two problems of on the cube". In: *Journal of Combinatorial Theory, Series A* (1992), pp. 142–146.

[7] Alan Hoffman. "Hoffman's ratio bound". In: *Linear Algebra and its Applications* (15 May 2021).

[8] Hao Huang. "Induced subgraphs of hypercubes and a proof of the Sensitivity Conjecture". In: *arXiv:1907.00847* (2019).

[9] Sophie Laplante, Reza Naserasr, and Anupa Sunny. "Sensitivity lower bounds from linear dependencies". In: *hal-02429358* (2020).

[10] M. Nisan and M. Szegedy. "On the degree of Boolean functions". In: *Computational Complexity* (1992), pp. 462–467.

[11] A. Potechin and Hing Yin Tsang. "A conjecture on induced subgraphs of Cayley graphs". In: *arXiv:2003.13166* (2020).

[12] D. Rubinstein. "Sensitivity vs. block sensitivity of boolean functions". In: *combinatorica 15(2)* (1995).

[13] Madars Virza. "Sensitivity versus block sensitivity of Boolean functions". In: *arXiv:1008.0521* (2010).

Statement of Authorship

I hereby declare that this document was composed by myself and thereby describes my own work, unless otherwise acknowledged within this document. Moreover, I assure to have read the *Satzung zur Wahrung guter wissenschaftlicher Praxis am Karlsruher Institut für Technologie (KIT)* hmm actually I didn't just yet.

David Schuldes, Karlsruhe, Date