wobei $(*)$ aus $\sqrt{a^2} = |a|$ für alle $a \in \mathbb{R}$ folgt.
(2) und (3):

$$\begin{aligned}
\|\boldsymbol{x}+\boldsymbol{y}\|^2 &= \langle \boldsymbol{x}+\boldsymbol{y}, \boldsymbol{x}+\boldsymbol{y}\rangle \\
&= \langle \boldsymbol{x},\boldsymbol{x}\rangle + \langle \boldsymbol{y},\boldsymbol{y}\rangle + 2\langle \boldsymbol{x},\boldsymbol{y}\rangle \\
&= \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 + 2\langle \boldsymbol{x},\boldsymbol{y}\rangle && \text{damit ist (3) bewiesen} \\
&\le \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 + 2\|\boldsymbol{x}\|\|\boldsymbol{y}\| && \text{Cauchy-Schwarz Ungleichung} \\
&= (\|\boldsymbol{x}\| + \|\boldsymbol{y}\|)^2 .
\end{aligned}$$

□

6.6 Die Lineare-Algebra-Methode

Eine einfache aber wichtige Folgerung aus dem Basisaustauschsatz von Steinitz ist die Tatsache, dass in jedem Vektorraum V höchstens $\dim V$ Vektoren linear unabhängig sein können.

Korollar 6.18: Dimensionsschranke
Sind $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ linear unabhängige Vektoren in einem linearen Raum der Dimension n, so gilt $m \le n$.

Diese Tatsache ist der Ausgangspunkt der sogenannten *Methode der linearen Algebra*, die bereits viele Anwendungen in der Diskreten Mathematik und in der Informatik gefunden hat.

Die allgemeine Idee dieser Methode ist die folgende: Um die Anzahl n der Elemente einer endlichen Menge $X = \{x_1, \ldots, x_n\}$ nach oben abzuschätzen, reicht es eine injektive Abbildung $f : X \to \mathbb{F}^d$ zu konstruieren, so dass die Vektoren $f(x_1), \ldots, f(x_n)$ linear unabhängig sind. Aus der Injektivität von f folgt $n \le |\mathbb{F}|^d$. Gelingt uns aber, die lineare Unabhängigkeit der Vektoren $f(x_1), \ldots, f(x_n)$ zu zeigen, so erhalten wir bereits exponentiell(!) bessere obere Schranke $n \le \dim \mathbb{F}^d = d$. Wir demonstrieren diese Methode an drei Beispielen. Unser erstes Beispiel scheint sehr spielerisch zu sein, es zeigt aber die Hauptidee der Methode.

Eine kleine Stadt namens »Eventown« (engl. »even« = »gerade«) hat n Einwohner. Da in der Stadt nicht viel los ist, haben die Einwohner eine Aktivität gefunden: Sie versuchen möglichst viele verschiedene Vereine zu bilden. Da zu viele Vereine schwer zu koordinieren sind, hat das Rathaus eine Regelung herausgegeben:

(i) die Anzahl der Mitglieder in jedem Verein muss *gerade* sein,
(ii) die Anzahl der gemeinsamen Mitglieder für je zwei Vereine muss *gerade* sein.

Wieviele Vereine können die Einwohner unter dieser Regelung bilden? Die Antwort ist einfach: Falls alle Einwohner verheiratet sind, können sie mindestens $2^{\lfloor n/2 \rfloor}$ Vereine bilden – es reicht, dass jeder Mann auch seine Frau mitnimmt. Das ist viel zu viel für eine so kleine Stadt! Um die Ordnung in der Stadt wieder herzustellen, ist das Rathaus gezwungen, die Anzahl der Vereine drastisch zu reduzieren. Es ist aber nicht erlaubt, die Regelung komplett umzuschreiben – erlaubt ist nur *ein einziges Wort* zu ändern.

Ein Einwohner hat den folgenden Vorschlag gemacht: Ersetze einfach das Wort »*gerade*« in (i) durch »*ungerade*«. Er behauptet, dass dann höchstens n verschiedene Vereine

gebildet werden können! Das Rathaus war von diesem Vorschlag so begeistert, dass es auch den Namen der Stadt von »Eventown« auf »Oddtown« geändert hat. Die Frage ist nun, ob diese Behauptung überhaupt stimmt?

Behauptung 6.19: »Oddtown«

Hat Oddtown n Einwohner, so können höchstens n Vereine gebildet werden.

Beweis:

Seien $A_1, \ldots, A_m \subseteq \{1, \ldots, n\}$ alle möglichen Vereine, die in Oddtown gebildet werden können. Formell sieht die neue Regelung folgendermaßen aus:

1. für alle i muss $|A_i|$ *ungerade* sein,
2. für alle $i \neq j$ muss $|A_i \cap A_j|$ *gerade* sein.

Wir wollen zeigen, dass dann $m \leq n$ gelten muss. Für einen Verein $A_i \subseteq \{1, \ldots, n\}$ sei $\boldsymbol{v}_i \in \{0,1\}^n$ sein Inzidenzvektor, d. h. $\boldsymbol{v}_i$ hat Einsen in Positionen j mit $j \in A_i$ und Nullen sonst. Wenn wir die Inzidenzvektoren als Vektoren über dem Körper $\mathbb{Z}_2$ betrachten, d. h. wenn wir modulo 2 rechnen, dann können wir die neuen Regeln so umschreiben:

$$\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = \begin{cases} 1 & \text{falls } i = j; \\ 0 & \text{falls } i \neq j. \end{cases}$$

Sei nun $\sum_{i=1}^{m} \lambda_i \boldsymbol{v}_i = \boldsymbol{0}$. Dann gilt für jedes $j = 1, \ldots, n$

$$0 = \langle \boldsymbol{0}, \boldsymbol{v}_j \rangle = \sum_{i=1}^{m} \lambda_i \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = \lambda_j \underbrace{\langle \boldsymbol{v}_j, \boldsymbol{v}_j \rangle}_{=1} = \lambda_j$$

und damit $\lambda_j = 0$ für alle j. Deshalb sind die Vektoren $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ linear unabhängig. Aus der Dimensionsschranke (Korollar 6.18) folgt daher die Ungleichung $m \leq \dim \mathbb{Z}_2^n = n$. □

Der folgende Satz zeigt eine eindrucksvollere Anwendung der Dimensionsschranke. Dieser Satz ist einer der Kernsätze in der sogenannten »Design Theory«. Den Spezialfall (für $k = 1$) hat R. A. Fisher im Jahre 1940 bewiesen.

Satz 6.20: Fisher's Ungleichung

Seien $A_1, \ldots, A_m$ verschiedene Teilmengen von $\{1, \ldots, n\}$ mit der Eigenschaft, dass je zwei Teilmengen die gleiche Anzahl gemeinsamer Elemente haben, d. h. für ein festes k und alle $i \neq j$ gilt $|A_i \cap A_j| = k$. Dann gilt $m \leq n$.

Beweis:

Diesmal arbeiten wir über dem Körper $\mathbb{R}$ der reellen Zahlen. Sind $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m \in \{0,1\}^n$ die Inzidenzvektoren von $A_1, \ldots, A_m$, so gilt $\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = |A_i \cap A_j|$. Unser Ziel ist zu zeigen, dass die Vektoren $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ linear unabhängig (über dem Körper $\mathbb{R}$) sind. Dann folgt die Behauptung $m \leq \dim \mathbb{R}^n = n$ aus der Dimensionsschranke (Korollar 6.18).

Wir führen einen Widerspruchsbeweis durch und nehmen an, dass die Inzidenzvektoren $\boldsymbol{v}_1, \ldots, \boldsymbol{v}_m$ linear abhängig sind. Dann gibt es reelle Zahlen $\lambda_1, \ldots, \lambda_m$ mit

$\sum_{i=1}^m \lambda_i \boldsymbol{v}_i = \mathbf{0}$ und $\lambda_i \neq 0$ für mindestens ein i. Weiterhin gilt

$$\langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle = \begin{cases} |A_i| & \text{falls } i = j; \\ k & \text{falls } i \neq j. \end{cases} \tag{6.4}$$

Aus $\langle \boldsymbol{x} + \boldsymbol{y}, \boldsymbol{z} \rangle = \langle \boldsymbol{z}, \boldsymbol{x} + \boldsymbol{y} \rangle = \langle \boldsymbol{x}, \boldsymbol{z} \rangle + \langle \boldsymbol{y}, \boldsymbol{z} \rangle$ und (6.4) folgt

$$\begin{aligned} 0 = \langle \mathbf{0}, \mathbf{0} \rangle &= \Big\langle \sum_{i=1}^m \lambda_i \boldsymbol{v}_i,\ \sum_{j=1}^m \lambda_j \boldsymbol{v}_j \Big\rangle \\ &= \sum_{i=1}^m \lambda_i^2 \langle \boldsymbol{v}_i, \boldsymbol{v}_i \rangle + \sum_{i=1}^m \sum_{\substack{j=1 \\ j \neq i}}^m \lambda_i \lambda_j \langle \boldsymbol{v}_i, \boldsymbol{v}_j \rangle \\ &= \sum_{i=1}^m \lambda_i^2 |A_i| + \sum_{i=1}^m \sum_{\substack{j=1 \\ j \neq i}}^m \lambda_i \lambda_j k && \text{wegen (6.4)} \\ &= \sum_{i=1}^m \lambda_i^2 (|A_i| - k) + k \cdot \Big(\sum_{i=1}^m \lambda_i \Big)^2 && \text{Umformung.} \end{aligned}$$

Es ist klar, dass $|A_i| \geq k$ für *alle* i gelten muss und $|A_i| = k$ für *höchstens ein* i gelten kann, da sonst die Eigenschaft $|A_i \cap A_j| = k$ verletzt wäre. Wir wissen auch, dass nicht alle Koeffizienten $\lambda_1, \ldots, \lambda_m$ gleich Null sind. Sind mindestens zwei von ihnen ungleich Null, so ist bereits die erste Summe ungleich Null. Ist nur ein Koeffizient ungleich Null, so muss die zweite Summe ungleich Null sein. In beiden Fällen erhalten wir einen Widerspruch. □

Unser nächstes Beispiel zeigt, dass man mit Hilfe der Dimensionsschranke nicht nur Aussagen über Mengen beweisen sondern auch einige »merkwürdige« Objekte konstruieren kann. Diesmal geht es um sogenannte »Ramsey-Graphen«.

Zur Erinnerung: Eine *Clique* in einem Graphen $G = (V, E)$ ist eine Teilmenge $S \subseteq V$ der Knoten, so dass zwischen je zwei Knoten in S eine Kante liegt. Eine *unabhängige Menge* in G ist eine Teilmenge $T \subseteq V$ der Knoten, so dass zwischen *keinen* zwei Knoten in T eine Kante liegt. Sei $r(G)$ die kleinste Zahl r, so dass der Graph G weder eine Clique noch eine unabhängige Menge mit r Knoten besitzt.

Graphen mit kleinem $r(G)$ sind sehr merkwürdige Objekte: Hat ein Graph G keine großen Cliquen, so muss er relativ wenige Kanten enthalten; dann sollte es aber eine große unabhängige Menge geben. Hat der Graph dagegen keine großen unabhängigen Mengen, so muss er viele Kanten und damit auch eine große Clique enthalten.

Nichtsdestotrotz gibt es Graphen G auf n Knoten mit $r(G) \leq 2 \log n$; solche Graphen sind als *Ramsey-Graphen* bekannt. Die Existenz solcher Graphen kann man mit Hilfe der sogenannten »Probabilistischen Methode« beweisen (siehe Abschnitt 12.4). Diese Methode zeigt aber nur die *Existenz* – bisher ist es nicht gelungen, mindestens einen Ramsey-Graphen *explizit* zu konstruieren. Heutzutage sind nur Konstruktionen von Graphen G mit $r(G) \leq n^\epsilon$ für bestimmte Konstanten $\epsilon < 1$ bekannt. Die meisten Konstruktionen benutzen die lineare Algebra, und wir demonstrieren dies an einem Beispiel.

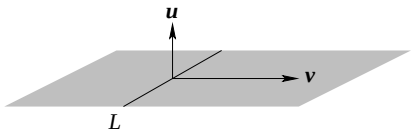

Bild 6.7: Für $\boldsymbol{u} = (0,0,c) \in \mathbb{R}^3$ ist $\boldsymbol{u}^\perp$ die Ebene $\{(x,y,0)\colon x,y \in \mathbb{R}\}$; ist $S = \{\boldsymbol{u},\boldsymbol{v}\}$ mit $\boldsymbol{v} = (a,0,0)$, so ist der Orthogonalraum $S^\perp$ genau die Gerade $L = \{(0,b,0)\colon b \in \mathbb{R}\}$.

Wir konstruieren den Graphen $G_n = (V,E)$ mit $n = \binom{t}{2}$ Knoten folgendermaßen. Als Knoten nehmen wir alle 3-elementigen Teilmengen von $\{1,\ldots,t\}$ und verbinden zwei Knoten A und B mit einer Kante genau dann, wenn $|A \cap B| = 1$ gilt.

Satz 6.21: Ramsey-Graphen

Der Graph G_n enthält weder eine Clique noch eine unabhängige Menge mit $3n^{1/3}$ Knoten.

Beweis:

Sei $A_1,\ldots,A_m$ eine Clique in G_n. Dann gilt $|A_i \cap A_j| = 1$ für alle $i \neq j$. Nach Fisher's Ungleichung muss dann $m \leq t$ gelten.

Sei nun $A_1,\ldots,A_m$ eine unabhängige Menge in G_n. Dann gilt $|A_i \cap A_j| \in \{0,2\}$ für alle $i \neq j$. D. h. alle $|A_i| = 3$ sind ungerade und alle $|A_i \cap A_j|$ mit $i \neq j$ sind gerade Zahlen. Das Oddtown-Beispiel sagt uns, dass auch in diesem Fall $m \leq t$ gelten muss.

Der Graph G_n hat also keine Cliquen oder unabhängigen Mengen der Größe $t+1$. Aus der Abschätzung $n = \binom{t}{2} \geq \left(\frac{t}{3}\right)^3$ (siehe Lemma 3.14) folgt $r(G) \leq t+1 \leq \sqrt[3]{9n} < 3n^{1/3}$. □

6.7 Orthogonalräume

In der Ebene $\mathbb{R}^2$ stehen zwei vom Nullvektor verschiedene Vektoren $\boldsymbol{x}$ und $\boldsymbol{y}$ senkrecht aufeinander (oder sind orthogonal), falls $\cos\alpha = 0$ für den Winkel α zwischen diesen Vektoren gilt, was wegen (6.3) und $\|\boldsymbol{x}\| > 0$, $\|\boldsymbol{y}\| > 0$ äquivalent zu $\langle \boldsymbol{x},\boldsymbol{y}\rangle = 0$ ist. Daher bezeichnet man zwei Vektoren $\boldsymbol{x}$ und $\boldsymbol{y}$ auch in $\mathbb{F}^n$ als *orthogonal*, wenn $\langle \boldsymbol{x},\boldsymbol{y}\rangle = 0$ gilt. Aus der Eigenschaften des Skalarprodukts folgt, dass die Menge

$$\boldsymbol{x}^\perp := \{\boldsymbol{y} \in \mathbb{F}^n\colon \langle \boldsymbol{x},\boldsymbol{y}\rangle = 0\}$$

der zu $\boldsymbol{x}$ orthogonalen Vektoren einen Vektorraum bildet: Sind $\boldsymbol{y},\boldsymbol{z} \in \boldsymbol{x}^\perp$ und $\lambda,\mu \in \mathbb{F}$, so gilt $\langle \lambda\boldsymbol{y} + \mu\boldsymbol{z},\boldsymbol{x}\rangle = \lambda\langle \boldsymbol{y},\boldsymbol{x}\rangle + \mu\langle \boldsymbol{z},\boldsymbol{x}\rangle = 0 + 0 = 0$. Dies lässt sich auch auf beliebige Teilmengen $S \subseteq \mathbb{F}^n$ erweitern: Die Menge

$$S^\perp := \{\boldsymbol{x} \in V\colon \langle \boldsymbol{x},\boldsymbol{y}\rangle = 0 \text{ für alle } \boldsymbol{y} \in S\}$$

bildet ebenfalls einen Vektorraum (siehe Bild 6.7), der *Orthogonalraum* oder *orthogonales Komplement* von S genannt wird.

Ist nun $V \subseteq \mathbb{F}^n$ ein Vektorraum, wie sieht dann $V^\perp$ aus? Sind die Mengen V und $V^\perp$ disjunkt? Nein, da der Nullvektor sowohl in V wie auch in $V^\perp$ enthalten ist. Nun