Komplexitätsklassen von Funktionen

Dissertation zur Erlangung des
naturwissenschaftlichen Doktorgrades
der Bayerischen Julius-Maximilians-Universität Würzburg

vorgelegt von

Heribert Vollmer

aus

Fredeburg

Würzburg, 1994

Eingereicht am: 26.10.93
bei der Fakultät für Mathematik
1. Gutachter: Prof. Dr. Klaus W. Wagner
2. Gutachter: Prof. Dr. Uwe Schöning
Tag der mündlichen Prüfung: 31.1.94

Ich danke allen, die mit Rat, Aufmunterung und Geduld zum Entstehen dieser Arbeit beigetragen haben, insbesondere meinem Doktorvater Klaus W. Wagner und meinen Kollegen Gerhard Buntrock, Ulrich Hertrampf, Krzysztof Loryś und Diana Rooß.

In der reinen Mathematik gehen wir von bestimmten Ableitungsregeln aus, nach denen wir folgern können, daß, *wenn* ein Satz wahr ist, *dann* auch ein zweiter Satz gilt. Diese Ableitungsregeln bilden den Hauptteil der Grundsätze formaler Logik. Wir wählen also irgendeine Hypothese, die uns amüsant erscheint, und leiten die entsprechenden Folgerungen ab. Gilt diese Hypothese für *irgend etwas* und nicht für eine oder mehrere Einzeltatsachen, dann stellen unsere Deduktionen Mathematik dar. Als Mathematik können wir also das Gebiet bezeichnen, auf dem wir nie wissen, wovon wir eigentlich reden und ob das, was wir sagen, auch wahr ist.

Bertrand Russell

Inhalt

Abbildungen und Tabellen:

1

Einleitung

Die strukturelle Komplexitätstheorie hat sich in den vergangenen 23 Jahren auf der Suche nach einer Lösung des bis heute offenen $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$-Problems zu einer reichen mathematischen Disziplin innerhalb der Theoretischen Informatik entwickelt. Ihr Gegenstandsbereich sind Komplexitätsklassen, d. h. durch verschiedene Berechnungsparadigmen – wie deterministische und nichtdeterministische Maschinen unter Ressourcenbeschränkungen – definierte Mengen von Problemen. Sie studiert strukturelle Eigenschaften dieser Klassen, charakterisiert sie auf verschiedene (evtl. sogar berechnungsunabhängige) Weise und versucht, ihre Beziehungen untereinander zu klären.

Die untersuchten Komplexitätsklassen waren lange Zeit überwiegend Klassen von Mengen. Um über ein konkretes Problem sprechen zu können, mußte dieses in eine Wortmenge kodiert werden. Das Problem des Handlungsreisenden beispielsweise besteht darin, zu einer Menge von zu besuchenden Städten und einer gegebenen Entfernungsmaxtrix die Länge der kürzesten Tour durch alle diese Städte zu finden. Dieses Problem wird typischerweise folgendermaßen in ein Ja/Nein-Problem umgeformt: Gegeben ist nun die Entfernungsmatrix und eine natürliche Zahl k; die Frage lautet: Ist die Länge der kürzesten Tour kleiner als k? Bekanntermaßen ist dieses Problem NP-vollständig. Mark Krentel untersuchte die ursprüngliche Version des Problems des Handlungsreisenden. Er faßte es mit ähnlich definierten Optimierungsproblemen zur Klasse Opt P zusammen [Kre88].

Opt P ist also eine Funktionenklasse; eine Funktion f gehört zu Opt P, falls es eine nichtdeterministische Polynomialzeit-Turingmaschine M gibt, die auf ihren Berechnungspfaden je einen Wert ausgibt, so daß für alle x die maximale Ausgabe (oder minimale Ausgabe) von M bei Eingabe x über alle Pfade gleich dem Wert $f(x)$ ist. Krentel zeigte, daß das oben definierte Problem vollständig für Opt P unter bestimmten Reduktionen, den sogenannten metrischen Reduktionen, ist. Interessant ist, daß Opt P eine bemerkenswerte Charakterisierung der Klasse $\mathrm{FP}^{\mathrm{NP}}$, der Klasse aller Funktionen, die deterministisch in Polynomialzeit mit einem Zugriff auf ein NP-Orakel berechnet werden können, erlaubt. Es gilt nämlich: $\mathrm{FP}^{\mathrm{NP}} = \mathrm{FP}^{\mathrm{Opt\,P}}[1]$, d.h. Funktionen aus $\mathrm{FP}^{\mathrm{NP}}$ sind genau die Funktionen, die geschrieben werden können als Komposition einer Opt P-Funktion und einer FP-Funktion. Aufgrund dieser Charakterisierung ergeben sich eine Reihe natürlicher vollständiger Probleme für die Klasse P^{NP}.

Seinosuke Toda führte im Jahre 1990 die Klasse Mid P ein [Tod90]. Mid P, ebenfalls eine Funktionenklasse, ist ähnlich definiert wie Opt P, nur wird hier nicht der maximale Wert aus der Menge der Ausgaben der nichtdeterministischen Maschine gewählt, sondern der mittlere. Ähnlich zu Krentels oben zitiertem Resultat gab Toda eine Charakterisierung der Klasse $\mathrm{FP}^{\mathrm{PP}}$ an, also der Klasse der Funktionen, die in Polynomialzeit berechenbar sind mit einem Orakel, das seinerseits probabilistisch in Polynomialzeit berechenbar ist: Sie umfaßt genau die Funktionen, die als Komposition einer Mid P-Funktion und einer FP-Funktion geschrieben werden können. Dieses Resultat erlaubt es, natürliche vollständige Probleme für $\mathrm{FP}^{\mathrm{PP}}$ und P^{PP} anzugeben. Toda fragte in seiner Arbeit nach ähnlichen Charakterisierungen von weiteren Klassen der Form $\mathrm{FP}^{(\cdot)}$.

Es wurden jedoch auch Funktionenklassen anderer Natur untersucht. Valiant führte 1979 die Klasse # P ein [Val79]. Eine Funktion f gehört zu # P, wenn es eine nichtdeterministische Polynomialzeit-Turingmaschine M gibt, so daß $f(x)$ gleich der Anzahl der akzeptierenden Pfade von M bei Eingabe x ist. Im Gegensatz dazu zählen span-P-Funktionen, eingeführt von Köbler, Schöning und Torán [KöScTo89], die Anzahl der verschiedenen Ausgabewerte solcher Maschinen. Gap-P-Funktionen schließlich ergeben die Anzahl der akzeptierenden Pfade vermindert um die Anzahl der verwerfenden Pfade. Sie wurden betrachtet von Fenner, Fortnow und Kurtz [FeFoKu91].

Es gibt enge Beziehungen zwischen den drei gerade genannten Klassen: Für eine beliebige Mengenklasse $\mathcal{K}$ ist die Klasse $\#\,\mathcal{K}$ definiert als die Klasse der Funktionen f, für die es eine Menge $A \in \mathcal{K}$ gibt, so daß $f(x)$ gleich der Anzahl der y aus einem bestimmten exponentiell großen Bereich ist, für die $(x, y) \in A$. Dann zeigt sich: span-P = # NP. Weiterhin wurde in [FeFoKu91] gezeigt, daß Gap-P genau aus den Funktionen besteht, die sich als Differenz zweier # P-Funktionen schreiben lassen: Gap-P = # P − # P.

Optimierungsklassen

Wir untersuchen zunächst Funktionenklassen der ersten Art: In Kapitel 3 starten wir mit der Feststellung, daß die Weise, Mediane zu bilden wie in der Definition der Klasse Mid P nicht die einzig mögliche und sinnvolle ist. Es ist u.E. natürlicher, das mittlere Element nicht aus der Menge der Ausgabewerte einer zugrundeliegenden Maschine zu wählen, sondern aus der geordneten Folge dieser Werte, in der jedes Element so oft vorkommt, wie es auf verschiedenen Pfaden ausgegeben wird. Die so gewonnene Funktionenklasse nennen wir Med P. Wir erarbeiten nun das Verhältnis der Medianklassen zueinander. Dazu betrachten wir noch eine dritte Art von Medianen, indem wir einen Operator $\mathrm{M\overline{ed}}$ einführen, der eine Mengenklasse in eine Funktionenklasse überführt. $\mathrm{M\overline{ed}}\,\mathrm{P}$ besteht aus den Funktionen f, für die eine Menge $A \in \mathrm{P}$ existiert, so daß $f(x)$ gleich dem mittleren Element der Menge aller y aus einem bestimmten exponentiell großen Bereich ist, für die $(x, y) \in A$. Intuitiv gesprochen berechnen $\mathrm{M\overline{ed}}\,\mathrm{P}$-Funktionen die Kodierung des mittleren akzeptierenden Pfades einer Turingmaschine wie oben. Analog wird $\mathrm{M\overline{ed}}\,\mathrm{NP}$ über Mengen $A \in \mathrm{NP}$ definiert.

Es zeigt sich nun, daß $\mathrm{M\overline{ed}}\,\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P}$ und $\mathrm{M\overline{ed}}\,\mathrm{P} \subseteq \mathrm{Mid}\,\mathrm{P} = \mathrm{M\overline{ed}}\,\mathrm{NP}$. Todas Arbeit zeigte, daß die Klasse Mid P eine ähnliche Komplexität wie die Klasse # P hat. Das genaue Verhältnis der Klassen zueinander blieb jedoch offen. Wir zeigen, daß # P eine Teilmenge von $\mathrm{M\overline{ed}}\,\mathrm{P}$ und span-P eine Teilmenge von Mid P ist. So kommen wir zu dem Inklusionsdiagramm auf Seite 29. Um zu zeigen, daß alle Klassen dieses Diagramms vermutlich verschieden voneinander sind, gehen wir folgendermaßen vor: Gegeben seien zwei Funktionenklassen, die zu trennen sind. Dann geben wir einen Operator an, der diese Klassen in Mengenklassen überführt, deren Verschiedenheit allgemein vermutet wird und eventuell durch die Existenz eines entsprechenden Orakels unterstützt wird. Wären also die Funktionenklassen gleich, so wären es – entgegen allgemeinem Glauben – auch die Mengenklassen. Auf diese Art und Weise zeigen wir, daß alle Klassen des Diagramms verschieden voneinander sind, es sei denn, es käme zu irgendwelchen unerwarteten Kollapsresultaten in verschiedenen Inklusionshierarchien von Mengenklassen, zum Beispiel dem Kollaps der Counting-Hierarchie [Wag86a, Tor88].

Auf der anderen Seite jedoch ist es möglich, analog zu Todas Satz eine Charakterisierung der Klasse $\mathrm{FP}^{\mathrm{PP}}$ auch mit Hilfe der anderen Medianklassen anzugeben. Die Medianklassen haben also, obwohl sie vermutlich verschieden voneinander sind, einige ähnliche Eigenschaften. Dies zeigt sich auch bei der Untersuchung vollständiger Probleme für diese Klassen. Aus der gerade angegebenen Übertragung von Todas Charakterisierung ergibt sich direkt, daß die Medianklassen die gleichen harten Probleme unter metrischen Reduktionen haben. Unter einem strengeren Reduktionsbegriff, den funktionalen many-one-Reduktionen (vgl. Seite 37), unter denen alle untersuchten Medianklassen abgeschlossen sind, gelingt es, die Probleme, von denen wir zunächst zeigten, daß sie hart sind für alle Klassen unter metrischen Reduktionen, genauer zu klassifizieren und Vollständigkeit für verschiedene Klassen zu zeigen.

Die Transformationen der Medianklassen in Mengenklassen, die im Diagramm auf Seite 31 dargestellt sind, werden mit dem Operator S durchgeführt. Ist $\mathcal{F}$ eine Funktionenklasse, so besteht die Mengenklasse $\mathrm{S} \cdot \mathcal{F}$ aus den Mengen A, für die Funktionen $f \in \mathcal{F}$ und $g \in \mathrm{FP}$ existieren, so daß $x \in A \iff f(x) \geq g(x)$. Die Klasse $\mathrm{S} \cdot \mathcal{F}$ hat eine Komplexität, die der der Klasse $\mathcal{F}$ sehr ähnlich ist, denn natürlich gilt stets $\mathrm{P}^{\mathcal{F}} = \mathrm{P}^{\mathrm{S}\cdot\mathcal{F}}$. Wir entnehmen also dem Diagramm, daß die Funktionenklasse Mid P eine Komplexität hat, die der der Mengenklasse $\mathrm{PP}^{\mathrm{NP}}$ entspricht. Ähnliches gilt für Med P und PP (und übrigens auch für Max P, die Teilmenge der Maximierungsfunktionen aus Opt P, und NP; sowie für Min P, die Minimierungsfunktionen aus Opt P, und co-NP). Geben wir beide Medianklassen als Orakel zu einer FP-Berechnung, so verschwindet der Unterschied: $\mathrm{FP}^{\mathrm{Med\,P}} = \mathrm{FP}^{\mathrm{Mid\,P}}$. Gleiches gilt für die Mengenseite: $\mathrm{FP}^{\mathrm{PP}} = \mathrm{FP}^{\mathrm{PP}^{\mathrm{NP}}}$; dies ist eine Folgerung aus dem Resultat, daß jede Zählfunktion mit einer Basismenge aus der Polynomialzeithierarchie metrisch reduzierbar ist auf eine # P-Funktion: $\#\,\mathrm{PH} \subseteq \mathrm{FP}^{\#\mathrm{P}}[1]$ [ToWa91]. Diese Beobachtung verhilft zu einer genaueren Einschätzung der Klasse Mid P, als dies bisher möglich war.

Bei der Klasse Mid P kommt also zur Medianbestimmung ein Existenzquantor; die Klasse Med P ist hingegen eine „reinere“ Mediananklasse. Wir werden uns daher in den folgenden Betrachtungen auf sie beschränken.

Aus den Arbeiten [Kre88] (vgl. auch [Köb89]) und [Tod90] sowie Kapitel 3 der vorliegenden Arbeit ergeben sich also die folgenden Resultate:

(A)	(B)
$\mathrm{FP}^{\mathrm{NP}} = \mathrm{FP}^{\mathrm{Max\,P}}[1]$	$\mathrm{S}\cdot\mathrm{Max\,P} = \mathrm{NP}$
$\mathrm{FP}^{\mathrm{co\text{-}NP}} = \mathrm{FP}^{\mathrm{Min\,P}}[1]$	$\mathrm{S}\cdot\mathrm{Min\,P} = \mathrm{co\text{-}NP}$
$\mathrm{FP}^{\mathrm{PP}} = \mathrm{FP}^{\mathrm{Med\,P}}[1]$	$\mathrm{S}\cdot\mathrm{Med\,P} = \mathrm{PP}$

Die Gegenüberstellung zeigt, daß die Klassen nicht nur Ähnlichkeiten in den Definitionen sondern wichtige gemeinsame Eigenschaften haben. Wir bemühen uns in Kapitel 5, diese Eigenschaften herauszuarbeiten und eine allgemeine Theorie von Optimierungsklassen zu entwickeln. Optimierung bedeutet dabei nicht nur Maximierung, sondern allgemeiner Auswahl eines Elements nach bestimmten Gütekriterien; sie kann also auch eine Minimierung oder eine Medianbildung sein.

Essentiell für die Beweise der unter (A) angegebenen Resultate ist die Möglichkeit, paralleles Erfragen mehrerer Funktionswerte durch eine einzige Frage nach einem Funktionswert zu simulieren, wie dies bei Opt P und auch bei Med P möglich ist. Diese Eigenschaft allein zeichnet Optimierungsklassen jedoch noch nicht gegenüber den Zählklassen aus, denn z. B. hat # P ebenfalls diese Eigenschaft. Optimierungsfunktionen sind jedoch wie oben erläutert gekennzeichnet durch einen Auswahlprozeß. Unterziehen wir nun jedes Element aus dem Bereich der Elemente, aus dem die Auswahl getroffen wird, einer arithmetischen Operation, die nicht vom Element selbst sondern nur von einer globalen Eingabe abhängt, so überträgt sich diese Operation unter bestimmten Voraussetzungen auf das Optimum. Betrachten wir als Beispiel eine Med P-Funktion h, die berechnet werde von der nichtdeterministischen Polynomialzeit-Maschine M, und eine FP-Funktion g. Wir definieren nun eine neue Maschine M', die bei einer Eingabe x zunächst M mit Eingabe x simuliert, aber dann auf jedem Pfad statt des Ausgabewertes von M nun das Minimum von diesem Wert und dem Wert $g(x)$ ausgibt. Der Median über alle Ausgabewerte von M' ist nun offensichtlich das Minimum von $g(x)$ und dem Median über die Ausgaben von M. Die Maschine M' belegt also, daß die Funktion $h'(x) =_{\text{def}} \min\{h(x), g(x)\}$ ein Element der Klasse Med P ist. Med P ist demnach abgeschlossen unter min-Operationen (und natürlich auch max-Operationen) mit FP-Funktionen. Eine Konstruktion wie die obige ist für # P nicht möglich. Abschluß von # P unter min-Operationen mit FP-Funktionen hätte schwerwiegende und unerwartete Konsequenzen.

Die Ergebnisse von Kapitel 5 zeigen, daß allein diese zwei Eigenschaften einer Funktionenklasse ausreichen, um eine Reihe interessanter Resultate zu beweisen. Wir nennen also eine Funktionenklasse, die (neben fünf kleineren technischen Anforderungen) die Simulation paralleler Fragen durch eine Frage erlaubt und unter min-max-Operationen mit FP-Funktionen abgeschlossen ist, eine *p-fundierte Klasse von Optimierungsfunktionen (PFO)* (vgl. Definition 5.4 auf Seite 59). Wir zeigen, daß FP diese Eigenschaften hat, und daß sich diese Eigenschaften übertragen bei der Konstruktion einer neuen Funktionenklasse aus einer gegebenen durch Bildung von Maxima, Minima und Medianen aus einem exponentiell großen Bereich von Werten einer Funktion der Ausgangsklasse; d. h. ist die Funktionenklasse $\mathcal{F}$ eine p-fundierte Klasse von Optimierungsfunktionen, so sind auch $\text{Max} \cdot \mathcal{F}$, $\text{Min} \cdot \mathcal{F}$ und $\text{Med} \cdot \mathcal{F}$ p-fundierte Klassen von Optimierungsfunktionen. (Es ist leicht zu sehen, daß Max P = Max · FP, Min P = Min · FP und Med P = Med · FP.)

Transformationen

Die oben unter (A) und (B) genannten Resultate stellen eine enge Beziehung zwischen Optimierungsklassen und Mengenklassen ähnlicher Komplexität her. Wir stellen uns allgemein die Frage: Gegeben eine beliebige Mengenklasse $\mathcal{K}$; was ist die $\mathcal{K}$ entsprechende Funktionenklasse? Dazu suchen wir Operatoren, die Transformationen zwischen Funktionenklassen und Mengenklassen durchführen, die leicht berechenbar sind und daher die Komplexität bei der Transformation nicht zu sehr verfälschen und sich im Kontext möglichst vieler interessanter Klassen invers zueinander verhalten. Als Transformationsoperator von der Funktionen- in die Mengenseite bietet sich der Operator S von oben an. Es stellt sich heraus, daß für die umgekehrte Richtung ein Operator geeignet ist, den wir F nennen und der in einer Reihe von Arbeiten der letzten Zeit [BuHa88, Wag90, AlWi90, Ogi91] implizit vorhanden ist. Das Operatorenpaar S/F hat folgende angenehme Eigenschaften:

1. Gehen wir mit S von der Funktionenseite zur Mengenseite, so verändern wir die Komplexität kaum (S ist mit nur einer Frage an eine Funktion der Ausgangsklasse berechenbar: $\mathrm{S} \cdot \mathcal{K} \subseteq \mathrm{P}^{\mathcal{K}}[1]$). Gehen wir von der Mengenseite zur Funktionenseite, ist die Situation etwas schlechter: F kann mittels binärer Suche berechnet werden, also ist stets $\mathrm{F} \cdot \mathcal{K} \subseteq \mathrm{FP}^{\mathcal{K}}$; demnach ist die Komplexität der Klasse $\mathrm{F} \cdot \mathcal{K}$ nicht zu sehr unterschiedlich von der der Ausgangsklasse $\mathcal{K}$, obwohl sie im allgemeinen leicht höher sein kann.

2. Aufgrund von Punkt 1 können wir also nicht erwarten, daß alle Funktionenklassen Fixpunkte des Kompositionsoperators $\mathrm{F} \cdot \mathrm{S}$ und alle Mengenklassen Fixpunkte von $\mathrm{S} \cdot \mathrm{F}$ sind. Es stellt sich jedoch heraus, daß alle Mengenklassen $\mathcal{K}$, die im wesentlichen nur unter many-one-Reduktionen abgeschlossen sind, Fixpunkte von $\mathrm{S} \cdot \mathrm{F}$ sind. Die leicht höhere Komplexität von $\mathrm{F} \cdot \mathcal{K}$ im Vergleich zu $\mathcal{K}$ kann also nicht genutzt werden, wenn nur ein Zugriff mit S auf sie möglich ist. Auf der anderen Seite werden wir sehen, daß $\mathrm{F} \cdot \mathrm{S}$ auf allen interessanten Funktionenklassen ein Hüllenoperator ist und daß Funktionenklassen genau dann Fixpunkte von $\mathrm{F} \cdot \mathrm{S}$ sind, wenn sie abgeschlossen sind unter einer Art von binärer Suche über den Funktionswerten von monoton fallenden Funktionen.

3. Die Operatoren F und S sind monoton. Daraus ergibt sich folgendes: Sind $\mathcal{F}_1$ und $\mathcal{F}_2$ Fixpunkte von $\mathrm{F} \cdot \mathrm{S}$ und stehen sie in Beziehung zu den Mengenklassen $\mathcal{K}_1$ und $\mathcal{K}_2$ (d.h. gilt $\mathrm{S} \cdot \mathcal{F}_1 = \mathcal{K}_1$ und $\mathrm{S} \cdot \mathcal{F}_2 = \mathcal{K}_2$ sowie $\mathrm{F} \cdot \mathcal{K}_1 = \mathcal{F}_1$ und $\mathrm{F} \cdot \mathcal{K}_2 = \mathcal{F}_2$), so folgt: $\mathcal{F}_1 \subseteq \mathcal{F}_2 \iff \mathcal{K}_1 \subseteq \mathcal{K}_2$, also insbesondere $\mathcal{F}_1 = \mathcal{F}_2 \iff \mathcal{K}_1 = \mathcal{K}_2$.

4. Die Konversionsoperatoren etablieren eine enge Beziehung zwischen den funktionentheoretischen Operatoren Max, Min und Med sowie den mengentheoretischen Operatoren $\exists$, $\forall$ und C, wie es in Spezialfällen oben unter (B) bereits angedeutet wurde.

5. Die Konversionsoperatoren übersetzen natürliche Abschlußeigenschaften von Funktionenklassen in natürliche Abschlußeigenschaften von Mengenklassen, und umgekehrt (vgl. Tabelle 5.1, Seite 73).

Abschlußeigenschaften

Ein Blick in die komplexitätstheoretische Literatur der letzten Jahre zeigt, daß eine Reihe berühmter Resultate nur von einigen wenigen Abschlußeigenschaften der betrachteten Klassen abhängt, nämlich Abschluß unter Vereinigung, Durchschnitt, disjunktiven Reduktionen und konjunktiven Reduktionen. Eine

Komplexitätsklasse, die die Klasse P umfaßt und die gerade angegebenen Abschlußeigenschaften besitzt, nennen wir *abstrakte Polynomialzeit-Komplexitätsklasse (APK)*. Die Aussagen, die in [Li93, Tor91, Sip83, Lau83, KSTT92, Tod91, BeReSp90, FoRe91, Her90, BeGiHe90, Kad87] für spezielle Klassen bewiesen wurden, sind tatsächlich allgemein gültig für abstrakte Polynomialzeit-Komplexitätsklassen oder für die Boolesche Hülle solcher Klassen. In der Theorie der formalen Sprachen spielt der Begriff „Abstrakte Sprachfamilie (AFL)“ eine ähnliche Rolle in dem Sinne, daß eine Reihe von Einzelresultaten bereits allgemein für Sprachklassen, die die AFL-Axiome erfüllen, gültig ist. Interessanterweise gibt es folgende Verbindung zwischen den beiden Begriffen: eine Mengenklasse ist genau dann eine abstrakte Sprachfamilie, die unter many-one-Reduktionen abgeschlossen ist, wenn sie eine abstrakte Polynomialzeit-Komplexitätsklasse ist, die unter $\exists$-Quantifizierung abgeschlossen ist.

Der oben genannte Punkt 5 kann nun folgendermaßen präzisiert werden: Die Operatoren S und F übersetzen genau die APK-Eigenschaften in eine etwas strengere Form der PFO-Eigenschaften und umgekehrt.

Polynomialzeit-Orakelberechnungen

Die Operatoren F und S erlauben es uns, Todas Frage nach einer allgemeinen Charakterisierung von Polynomialzeit-Orakelberechnungen elegant zu beantworten. Wir zeigen in Abschnitt 5.3, daß für eine PFO $\mathcal{F}$ schon binäre Suche und Subtraktion ausreichen, um $\mathrm{FP}^{\mathcal{F}}$-Berechnungen zu simulieren:

$$\mathrm{FP}^{\mathcal{F}} = \mathrm{FS}\cdot\mathcal{F} - \mathrm{FS}\cdot\mathcal{F}.$$

Weiterhin ergibt sich allgemein für PFOs $\mathcal{F}$ und APKs $\mathcal{K}$:

$$\begin{aligned}\mathrm{FP}^{\mathcal{F}} &= \mathrm{FP}^{\mathrm{FS}\cdot\mathcal{F}}[1]\\ \mathrm{FP}^{\mathcal{K}} &= \mathrm{FP}^{\mathrm{F}\cdot\mathcal{K}}[1]\end{aligned}$$

Wir charakterisieren also $\mathrm{FP}^{\mathcal{F}}$ als Klasse der Funktionen, die sich als Komposition einer $\mathrm{FS}\cdot\mathcal{F}$-Funktion und einer FP-Funktion schreiben lassen, und $\mathrm{FP}^{\mathcal{K}}$ als Klasse der Funktionen, die sich als Komposition einer $\mathrm{F}\cdot\mathcal{K}$-Funktion und einer FP-Funktion schreiben lassen.

In Erweiterung eines Resultats aus [Ogi91] ergibt sich: Die Klasse $\mathrm{P}^{\mathcal{K}}$ (bzw. $\mathrm{P}^{\mathcal{F}}$) läßt sich charakterisieren als Klasse der Sprachen A, für die eine $\mathrm{F}\cdot\mathcal{K}$-Funktion (bzw. $\mathrm{FS}\cdot\mathcal{F}$-Funktion) h existiert, so daß ein Wort x genau dann zu A gehört, wenn die Funktion h an der Stelle x einen ungeraden Wert annimmt.

Fixpunkte

Obwohl wir nicht allgemein von Funktionenklassen erwarten können, daß sie Fixpunkte von $\mathrm{F} \cdot \mathrm{S}$ sind, gelingt es doch, erstaunlich viele Fixpunkte zu identifizieren. Wir zeigen, daß unter geringen zusätzlichen Anforderungen an eine PFO $\mathcal{F}$ alle Klassen der Hierarchie, die aus $\mathcal{F}$ entsteht durch endlich-oftmalige Anwendung der Operatoren Max, Min und $\mathrm{FP}^{(\cdot)}$ (der Min-Max-Hierarchie), Fixpunkte von $\mathrm{F} \cdot \mathrm{S}$ sind und genau den Klassen der Polynomialzeithierarchie über der Mengenklasse $\mathrm{S} \cdot \mathcal{F}$ entsprechen. Aufgrund von Punkt 3 oben folgt also, daß zwei Klassen der Min-Max-Hierarchie über $\mathcal{F}$ genau dann zusammenfallen, wenn die entsprechenden Klassen der Polynomialzeithierarchie über $\mathrm{S} \cdot \mathcal{F}$ zusammenfallen. Weiterhin beweisen wir die folgenden strukturellen Aussagen (vgl. Bild 5.2, Seite 88): Die $\mathrm{FP}^{(\cdot)}$-Klassen bestehen aus genau den Funktionen, die sich als Differenz von Funktionen aus den darunterliegenden Min-Klassen (oder Max-Klassen) schreiben lassen. Die Max-Klassen bestehen aus genau den Funktionen, die sich als Differenz einer FP-Funktion und einer Funktion der Min-Klasse der gleichen Stufe schreiben lassen (und umgekehrt). Die $\mathrm{FP}^{(\cdot)}$-Klassen sind in den nächsthöheren Min- und Max-Klassen enthalten. Die Vereinigung aller Klassen der Min-Max-Hierarchie ist der Abschluß der Basisklasse unter Min und Max oder Min und Subtraktion oder Max und Subtraktion.

Auf ähnliche Weise untersuchen wir eine Hierarchie über Klassen $\mathcal{F}$, die mit den Operatoren Med und $\mathrm{FP}^{(\cdot)}$ gebildet wird, zeigen Verbindungen zur Counting-Hierarchie über $\mathrm{S} \cdot \mathcal{F}$ auf und geben ähnliche strukturelle Resultate wie oben an (vgl. Bild 5.3, Seite 91).

Zählklassen

In Kapitel 6 wenden wir uns Funktionenklassen der zweiten Art, also den Zählklassen, zu. Ein Blick in die Literatur zeigt, daß die meisten Aussagen über die vielleicht bekannteste Zählklasse $\#\mathrm{P}$ von drei Abschlußeigenschaften abhängen: Abschluß unter exponentieller Summation, polynomieller Multiplikation und polynomieller Auswahl. Eine Funktionenklasse, die (neben einigen kleineren technischen Anforderungen) diese drei Abschlußeigenschaften hat, nennen wir *p-fundierte Klasse von Zählfunktionen (PFZ).*

Es ergeben sich interessante Beziehungen zu den oben angegebenen Begriffen: Ist $\mathcal{K}$ eine APK, so sind $\#\mathcal{K}$ und $\#\mathcal{K} - \#\mathcal{K}$ p-fundierte Klassen von Zählfunktionen. Ist $\mathcal{F}$ eine PFO, so ist die Funktionenklasse, deren Elemente durch eine bestimmte Form von Summation aus Funktionen aus $\mathcal{F}$ entstehen, eine p-fundierte Klasse von Zählfunktionen. Unter bestimmten zusätzlichen Annahmen werden p-fundierte Klassen von Zählfunktionen unter dem Operator S in abstrakte Polynomialzeit-Komplexitätsklassen überführt. Auch im Kontext von

Zählklassen finden wir ein Operatorenpaar (# und U), das die Eigenschaft hat, daß sehr viele Zählklassen Fixpunkte des Kompositionsoperators $\# \cdot \mathrm{U}$ sind. Schließlich charakterisieren wir die Hierarchie der Zählfunktionen über einer p-fundierten Zählklasse $\mathcal{F}$, also die Klassen $\mathcal{F}$, $\#\,\mathrm{P}^{\mathcal{F}}$, $\#\,\mathrm{P}^{\#\,\mathrm{P}^{\mathcal{F}}}$, ..., mit Hilfe der Operatoren Summation und modifizierte Differenz. Die Vereinigung all dieser Klassen ist genau der Abschluß der Klasse $\mathcal{F}$ unter Summation und modifizierter Differenz.

Anwendungen

In Kapitel 7 demonstrieren wir die Anwendbarkeit der von uns entwickelten Theorie, indem wir Resultate aus den Arbeiten [KöScTo89, Tor88, Köb89, OgHe93, ThToWa93] verbessern und verallgemeinern.

2

Grundlagen

Wir vereinbaren in diesem Kapitel die für die vorliegende Arbeit grundlegenden Definitionen und Notationen. Wir erwarten Grundkenntnisse des Lesers über Mengen, Turing-Maschinen, Reduzierbarkeiten und Komplexitätsklassen.

Sprachen, Mengen, Funktionen

Für ein Alphabet Σ bezeichnen wir mit Σ^* das freie Monoid über Σ, also die Menge aller Wörter über Σ. Das leere Wort notieren wir mit ε und die Konkatenation von Wörtern u und v mit $u \cdot v$. Die Länge eines Wortes $w \in \Sigma^*$ wird mit $|w|$ bezeichnet. Eine Teilmenge von Σ^* nennen wir auch Sprache über Σ.

Für eine Sprache A bezeichnen wir mit c_A die charakteristische Funktion von A. Für eine Klasse von Sprachen $\mathcal{K}$ ist $\mathrm{char}(\mathcal{K}) =_{\mathrm{def}} \{\, c_A \mid A \in \mathcal{K} \,\}$. Die Kardinalität einer Sprache (oder auch beliebigen Menge) M bezeichnen wir mit $|M|$ oder mit $\# M$. Für Sprachen A und B bezeichnet $A \oplus B$ die markierte Vereinigung, also $A \oplus B =_{\mathrm{def}} 0 \cdot A \cup 1 \cdot B$.

Die Menge der natürlichen Zahlen bezeichnen wir mit $\mathbb{N}$, die der ganzen Zahlen mit $\mathbb{Z}$. Für $y \in \mathbb{N}$ ist $[y] =_{\mathrm{def}} \{-y+1, -y+2, \ldots, y\}$. Für $z \in \mathbb{Z}$ ist $\mathrm{sign}(z)$ das Vorzeichen von z. Für eine rationale Zahl x sei $\lfloor x \rfloor =_{\mathrm{def}} \max\{\, n \in \mathbb{Z} \mid n \leq x \,\}$ und $\lceil x \rceil =_{\mathrm{def}} \min\{\, n \in \mathbb{Z} \mid n \geq x \,\}$. Modifizierte Subtraktion bezeichnen wir mit $\dot{-}$. Wir benutzen folgende auf die ganzen Zahlen erweiterte Definition der modifizierten Subtraktion: $a \dot{-} b =_{\mathrm{def}} \max\{0, a-b\}$, falls $a \geq 0$; und $a \dot{-} b =_{\mathrm{def}} \min\{0, a-b\}$, falls $a < 0$. Für $a, b \geq 0$ bezeichnet also unser $\dot{-}$ die gewöhnliche modifizierte Subtraktion, also das, was Ogiwara und Hemachandra [OgHe93] mit $\ominus$ notieren. Wir verallgemeinern die ursprüngliche Definition, weil wir generell Operationen über den ganzen Zahlen betrachten. Unsere Wahl fiel dabei auf die obige Definition, weil sie die wünschenswerte Eigenschaft hat, daß der Abschluß einer Funktionenklasse (mit möglicherweise negativen Funktionen) unter modifizierter Subtraktion auch die Klasse selbst wieder enthält (denn es ist stets $a \dot{-} 0 = a$), und weil sie unter allen Erweiterungen mit der gerade genannten Eigenschaft sich durch eine besondere Natürlichkeit und Einfachheit auszeichnet. Ganzzahlige Division bezeichnen wir mit $\div$, also $a \div b =_{\mathrm{def}} \lfloor \frac{a}{b} \rfloor$. $a \bmod b$ bezeichnet die Zahl r, so daß $a = b \cdot (a \div b) + r$. Wir verwenden folgende Definition des Binomialkoeffizienten: Seien $x, y \in \mathbb{Z}$, $y \geq 0$. Dann ist

$$\binom{x}{y} =_{\mathrm{def}} \frac{x(x-1)(x-2)\cdots(x-y+1)}{1 \cdot 2 \cdots y},$$

für $y \neq 0$, und $\binom{x}{0} =_{\mathrm{def}} 1$.

Die Menge aller Polynome bezeichnen wir mit Pol. Komposition von Funktionen bezeichnen wir mit $\circ$; $(f \circ g)(x) =_{\mathrm{def}} f(g(x))$. Für Mengen von Funktionen $\mathcal{F}$ und $\mathcal{F}'$ und eine Operation op auf Funktionen, z. B. op $\in \{+, -, \cdot, \dot{-}\}$, definieren wir $\mathcal{F}$ op $\mathcal{F}' =_{\mathrm{def}} \{ f \text{ op } f' \mid f \in \mathcal{F}, f' \in \mathcal{F}' \}$. Den Abschluß einer Menge $X \subseteq M$ unter einer Menge von Operationen Ω auf M bezeichnen wir mit $\Gamma_\Omega(X)$.

Wir verwenden das Berechnungsmodell der (deterministischen oder nichtdeterministischen) polynomiell zeitbeschränkten Turingmaschine. Turingmaschinen arbeiten definitionsgemäß auf Zeichenfolgen. Wenn wir also davon reden wollen, daß Turingmaschinen zahlentheoretische Funktionen berechnen, setzen wir dabei eine Kodierung von Zahlen in Wörter über unserem Standardalphabet $\{0, 1\}$ voraus. Wir legen uns im folgenden nicht auf eine konkrete Kodierung fest; wir fordern lediglich, daß sie die ganzen Zahlen eineindeutig den Wörtern über $\{0, 1\}$ zuordnet, daß die Länge der Kodierung einer Zahl n über $\{0, 1\}$ und der Logarithmus von n polynomiell verknüpft sind und daß alle arithmetischen Operationen, die mit gebräuchlichen Kodierungen in Polynomialzeit durchführbar sind, auch bei unserer Kodierung nicht mehr als Polynomialzeit beanspruchen.

Es wird sich im Laufe der Arbeit herausstellen, daß wir oft eine Kodierung einer Folge ganzer Zahlen in eine natürliche Zahl benötigen. Dazu verwenden wir folgendes Schema: Seien $m, y \in \mathbb{N}$ und $u_1, u_2, \ldots, u_m \in \mathbb{Z}$ gegeben; dann definieren wir:

$$\langle u_1, u_2, \ldots, u_m \rangle_y =_{\mathrm{def}} \sum_{i=1}^{m} (u_i + y) \cdot (2y)^{i-1} - 1.$$

Auf diese Weise wird die Menge der endlichen Folgen von Elementen aus $[y]$ bijektiv auf $\mathbb{N}$ abgebildet wie in Abbildung 2.1 wiedergegeben. Für gegebene $U, y \in \mathbb{N}$ gibt es also genau eine Zerlegung $m \in \mathbb{N}$, $u_1, \ldots, u_m \in [y]$, so daß $\langle u_1, u_2, \ldots, u_m \rangle_y = U$. Offensichtlich kann diese Bijektion in deterministischer Polynomialzeit ausgeführt sowie auch invertiert werden. Wir werden im folgenden manchmal, falls keine Unklarheit entstehen kann, den Index zu den Klammern $\langle \cdots \rangle$ weglassen.

$$\begin{array}{rcl}
\langle -y+1\rangle_y & \mapsto & 0 \\
\langle -y+2\rangle_y & \mapsto & 1 \\
 & \ldots & \\
\langle y\rangle_y & \mapsto & 2y-1 \\
\langle -y+1,-y+1\rangle_y & \mapsto & 2y \\
\langle -y+2,-y+1\rangle_y & \mapsto & 2y+1 \\
 & \ldots & \\
\langle y,-y+1\rangle_y & \mapsto & 4y-1 \\
\langle -y+1,-y+2\rangle_y & \mapsto & 4y \\
\langle -y+2,-y+2\rangle_y & \mapsto & 4y+1 \\
 & \ldots & \\
\langle y,-y+2\rangle_y & \mapsto & 6y-1 \\
\langle -y+1,-y+3\rangle_y & \mapsto & 6y \\
\langle -y+2,-y+3\rangle_y & \mapsto & 6y+1 \\
 & \ldots & \\
\langle y,y\rangle_y & \mapsto & 2y+(2y)^2-1 \\
\langle -y+1,-y+1,-y+1\rangle_y & \mapsto & 2y+(2y)^2 \\
 & \ldots &
\end{array}$$

Abbildung 2.1: Erläuterung der Kodierung

Wir führen noch Bezeichnungen für die einzelnen Bestandteile der Zerlegung eines Paares U, y ein: Sei $\langle u_1, u_2, \ldots, u_m\rangle_y = U$, $u_1, u_2, \ldots, u_m \in [y]$, dann definieren wir

$$[U, y, i] =_{\text{def}} \begin{cases} u_i, & \text{falls } i \in \{1, \ldots, m\} \\ 0, & \text{sonst} \end{cases}$$

und

$$m[U, y] =_{\text{def}} m.$$

Es wird sich weiterhin herausstellen, daß wir ein zusätzliches Kodierungsschema benötigen, bei dem ebenfalls eine Folge von ganzen Zahlen in eine natürliche Zahl kodiert wird, aber diesmal unterscheiden sich die Elemente mit geradem Index von denen mit ungeradem Index bezüglich des zulässigen Wertebereiches. Für $m, y, z \in \mathbb{N}$ und $u_1, u_2, \ldots, u_{2m} \in \mathbb{Z}$ definieren wir

$$\langle u_1, \ldots, u_{2m}\rangle_{y,z} =_{\text{def}} \sum_{i=1}^{m} [(u_{2i-1} + y) \cdot (2y)^{i-1}(2z)^{i-1} + (u_{2i} + z) \cdot (2y)^{i}(2z)^{i-1}] - 1$$

Diese Kodierung hat ähnliche Eigenschaften wie die aus Abbildung 2.1. Sie ist eineindeutig (der Einfachheit halber wurde jedoch auf Surjektivität verzichtet, da diese später nicht benötigt wird), d. h. es gilt: Für gegebene U, y, z aus dem

Bildbereich der Kodierung gibt es genau eine Zerlegung $m \in \mathbb{N}$, $u_1, \ldots, u_{2m}$, so daß $u_1, u_3, \ldots, u_{2m-1} \in [y]$, $u_2, u_4, \ldots, u_{2m} \in [z]$ und $\langle u_1, \ldots, u_{2m} \rangle_{y,z} = U$. Auch hier sind offenbar Kodierung und Dekodierung in Polynomialzeit durchführbar. Wir werden auch hier in eindeutigen Fällen mitunter auf die Indizes verzichten.

Komplexitätsklassen, Reduktionen

Die komplexitätstheoretische Notation, die wir verwenden, folgt weitverbreitetem Standard [Sch86, WaWe86]. In Polynomialzeit durchführbare Turing-Reduzierbarkeit bezeichnen wir mit $\leq_T^{\mathrm{p}}$. In Polynomialzeit durchführbare many-one-Reduzierbarkeit bezeichnen wir mit $\leq_m^{\mathrm{p}}$. In Polynomialzeit durchführbare truth-table-Reduzierbarkeit bezeichnen wir mit $\leq_{tt}^{\mathrm{p}}$. Ist der Schaltkreis, der das Ergebnis der Reduktion aus den Antworten des Orakels berechnet, ein (unbounded fan-in) Oder-Gatter, so sprechen wir von disjunktiver Reduzierbarkeit; sie wird mit $\leq_{dtt}^{\mathrm{p}}$ notiert. Im Falle eines Und-Gatters handelt es sich um konjunktive Reduzierbarkeit; $\leq_{ctt}^{\mathrm{p}}$. Besteht der Schaltkreis nur aus Und- und Oder-Gattern (ist also monoton), so sprechen wir von positiver truth-table-Reduzierbarkeit; $\leq_{ptt}^{\mathrm{p}}$. Hat der monotone Schaltkreis konstante Tiefe (bounded depth), so schreiben wir $\leq_{bd\text{-}ptt}^{\mathrm{p}}$. Für einen Reduktionstyp $\leq_y^x$, eine Menge A und eine Klasse von Mengen $\mathcal{K}$ definieren wir $\mathcal{R}_y^x(A) =_{\mathrm{def}} \{\, B \mid B \leq_y^x A \,\}$ und $\mathcal{R}_y^x(\mathcal{K}) =_{\mathrm{def}} \bigcup_{B \in \mathcal{K}} \mathcal{R}_y^x(B)$. $\mathcal{K}$ heißt unter $\leq_y^x$ abgeschlossen, falls $\mathcal{K} = \mathcal{R}_y^x(\mathcal{K})$.

FP bezeichnet die Klasse aller Funktionen, die in Polynomialzeit auf einer deterministischen Turingmaschine berechnet werden können. FP_+ bezeichnet die Klasse aller Funktionen aus FP, die überall nicht-negativ sind.

Sind $\mathcal{K}_1$ und $\mathcal{K}_2$ Komplexitätsklassen, so definieren wir co-$\mathcal{K}_1 =_{\mathrm{def}} \{\, \overline{A} \mid A \in \mathcal{K}_1 \,\}$, $\mathcal{K}_1 \wedge \mathcal{K}_2 =_{\mathrm{def}} \{\, A \cap B \mid A \in \mathcal{K}_1, B \in \mathcal{K}_2 \,\}$ und $\mathcal{K}_1 \vee \mathcal{K}_2 =_{\mathrm{def}} \{\, A \cup B \mid A \in \mathcal{K}_1, B \in \mathcal{K}_2 \,\}$. Die *Boolesche Hierarchie* über $\mathcal{K}_1$ wird definiert als der Abschluß von $\mathcal{K}_1$ unter den genannten drei Operationen. $\mathrm{BH}(\mathcal{K}_1)$ ist die Vereinigung aller Klassen der Booleschen Hierarchie über $\mathcal{K}_1$.

Im Laufe der Arbeit werden wir eine Reihe von Operatoren untersuchen, die angewandt auf Komplexitätsklassen von Funktionen oder von Mengen neue Klassen bilden. Die mengentheoretischen Operatoren, die wir verwenden, sind seit längerer Zeit bekannt und gut untersucht [Wra77, Val79, Wag86a, Tor91].

Die Operatoren, mit denen wir beginnen, sind die Bausteine der Polynomialzeithierarchie, nämlich der Existenzquantor und der Universalquantor.

$$
\begin{array}{lcl}
A \in \exists\mathcal{K} & \iff & \text{es existieren } B \in \mathcal{K},\ g \in \mathrm{FP}, \text{ so daß} \\
 & & x \in A \iff (\exists y)(0 \leq y \leq g(x) \wedge (x, y) \in B). \\
A \in \forall\mathcal{K} & \iff & \text{es existieren } B \in \mathcal{K},\ g \in \mathrm{FP}, \text{ so daß} \\
 & & x \in A \iff (\forall y)(0 \leq y \leq g(x) \Rightarrow (x, y) \in B)\ .
\end{array}
$$

Die Klassen der Polynomialzeithierarchie über einer Mengenklasse $\mathcal{K}$ sind nun wie folgt definiert: $\Sigma_0^p \cdot \mathcal{K} = \Pi_0^p \cdot \mathcal{K} = \Delta_0^p \cdot \mathcal{K} = \mathcal{K}$, $\Sigma_{k+1}^p \cdot \mathcal{K} = \exists \Pi_k^p \cdot \mathcal{K}$, $\Pi_{k+1}^p \cdot \mathcal{K} = \forall \Sigma_k^p \cdot \mathcal{K}$ und $\Delta_{k+1}^p \cdot \mathcal{K} = \mathrm{P}^{\Sigma_k^p \cdot \mathcal{K} \cup \Pi_k^p \cdot \mathcal{K}}$. Die Klasse $\mathrm{PH} \cdot \mathcal{K}$ ist die Vereinigung aller Klassen der Polynomialzeithierarchie, also da die Sigma- und Pi-Klassen stets in den nächsthöheren Delta-Klassen enthalten sind: $\mathrm{PH} \cdot \mathcal{K} = \bigcup_{k \geq 0} \Delta_k^p \cdot \mathcal{K}$. Man beachte, daß die Delta-Klassen nicht unbedingt in den nächsten Sigma- oder Pi-Klassen enthalten sein müssen. (Es gibt sogar explizite Gegenbeispiele.) Für den Fall $\mathcal{K} = \mathrm{P}$ schreiben wir abkürzend $\Sigma_k^p = \Sigma_k^p \cdot \mathrm{P}$, $\Pi_k^p = \Pi_k^p \cdot \mathrm{P}$, $\Delta_k^p = \Delta_k^p \cdot \mathrm{P}$ und $\mathrm{PH} = \mathrm{PH} \cdot \mathrm{P}$.

Der nächste Operator verallgemeinert die Definition von Valiants Klasse $\#\mathrm{P}$ für beliebige Basisklassen $\mathcal{K}$:

$$f \in \# \cdot \mathcal{K} \iff \text{es existieren } B \in \mathcal{K},\ g \in \mathrm{FP}, \text{ so daß } f(x) = \#\{\, y \mid 0 \leq y \leq g(x) \wedge (x, y) \in B \,\}.$$

Offensichtlich ist $\# \cdot \mathrm{P} = \#\mathrm{P}$. Man beachte jedoch, daß für höhere Klassen $\mathcal{K}$ das, was wir gemäß obiger Definition unter $\# \cdot \mathcal{K}$ verstehen, nicht unbedingt gleich dem ist, was Valiant in [Val79] mit $\#\mathcal{K}$ bezeichnet. Wenn Valiant (und in seiner Tradition auch [KöScTo89, Tor88, Köb89]) $\#\mathcal{K}$ schreiben, ist diejenige Klasse gemeint, die wir hier mit $\#\mathrm{P}^{\mathcal{K}}$ notieren.

In den historischen Definitionen der obigen Operatoren findet man unsere Bedingung $0 \leq y \leq g(x)$ für ein $g \in \mathrm{FP}$ ersetzt durch $|y| \leq p(|x|)$ für ein $p \in \mathrm{Pol}$. Es zeigt sich jedoch, daß dies in allen Fällen, die uns interessieren, keinen Unterschied in den Resultaten ergibt. Wir wählten die angegebene Formulierung, da wir oft Wörter als Zahlen interpretieren und sie uns in diesem Kontext natürlich erschien. Wir bemerken, daß wir ebenfalls ohne Änderung der folgenden Resultate auch $g_1(x) \leq y \leq g_2(x)$ für zwei Funktionen $g_1, g_2 \in \mathrm{FP}$ hätten verlangen können. Wir werden im folgenden oft die abkürzende Schreibweise $y \leq g(x)$ verwenden und meinen stets $0 \leq y \leq g(x)$.

Funktionenklassen der Form $\#\mathcal{K}$ erlauben eine einfache Definition des Zählquantors:

$$A \in \mathrm{C}\mathcal{K} \iff \text{es existieren } f \in \#\mathcal{K},\ g \in \mathrm{FP}, \text{ so daß } x \in A \iff f(x) \geq g(x).$$

Bekannterweise ist $\mathrm{C} \cdot \mathrm{P} = \mathrm{PP}$ [Sim75, Gil77, Wag86a].

Die Counting-Hierarchie über einer Klasse $\mathcal{K}$ entsteht durch endlich-oftmalige Anwendung von Existenz-, Universal- oder Zählquantor auf $\mathcal{K}$, d.h. sie ist die kleinste Familie von Klassen, die $\mathcal{K}$ enthält und abgeschlossen ist under $\exists$, $\forall$ und C. $\mathrm{CH} \cdot \mathcal{K}$ ist die Vereinigung aller Klassen der Counting-Hierarchie über $\mathcal{K}$, und $\mathrm{CH} = \mathrm{CH} \cdot \mathrm{P}$. Da unabhängig von den Eigenschaften von $\mathcal{K}$ stets $\exists\mathcal{K} \cup \forall\mathcal{K} \subseteq \mathrm{C}\mathcal{K}$ gilt [Tor91], folgt also: $\mathrm{CH} \cdot \mathcal{K} = \bigcup_{k \geq 0} \mathrm{C}^k \cdot \mathcal{K}$.

Wagner [Wag86b] führte als Erweiterung der Klasse $\#\,\mathrm{P}$ die Hierarchie der Zählfunktionen ein. Sie besteht aus den Klassen

$$0\,\#\,\mathrm{P} =_{\mathrm{def}} \mathrm{FP} \text{ und } (i+1)\,\#\,\mathrm{P} =_{\mathrm{def}} \#\,\mathrm{P}^{i\,\#\,\mathrm{P}} \text{ für } i \geq 0.$$

FCH ist die Vereinigung aller Klassen der Hierarchie der Zählfunktionen.

Neben #-Klassen wurden weitere Klassen von Zählfunktionen in der Literatur untersucht:

Köbler, Schöning und Torán führten die Klasse span-P ein. Eine Funktion f gehört genau dann zu span-P, wenn eine nichtdeterministische polynomiell zeitbeschränkte Turingmaschine M existiert, so daß $f(x)$ gleich der Anzahl der verschiedenen Ausgabewerte über alle Pfade von M bei Eingabe x ist [KöScTo89].

Fenner, Fortnow und Kurtz führten die Klasse Gap-P ein. Eine Funktion f gehört genau dann zu Gap-P, wenn eine nichtdeterministische polynomiell zeitbeschränkte Turingmaschine M existiert, so daß $f(x)$ gleich der Anzahl der akzeptierenden Pfade von M bei Eingabe x vermindert um die Anzahl der verwerfenden Pfade von M bei Eingabe x ist [FeFoKu91].

Es ist folgendes bekannt [KöScTo89, Köb89, Sparta91, FeFoKu91]:

1. $\text{Gap-P} = \#\,\mathrm{P} - \#\,\mathrm{P} = \#\,\mathrm{P} - \mathrm{FP}$.
2. $\text{span-P} = \#\,\mathrm{NP} \subseteq \#\,\text{co-NP} = \#\,\mathrm{P}^{\mathrm{NP}} \subseteq \#\,\mathrm{NP} - \mathrm{FP} = \#\,\text{co-NP} - \mathrm{FP} = \#\,\mathrm{P}^{\mathrm{NP}} - \mathrm{FP} = \mathrm{FP} - \#\,\mathrm{NP} = \mathrm{FP} - \#\,\text{co-NP} = \mathrm{FP} - \#\,\mathrm{P}^{\mathrm{NP}} = \#\,\mathrm{NP} - \#\,\mathrm{NP} = \#\,\text{co-NP} - \#\,\text{co-NP} = \text{Gap-P}^{\mathrm{NP}}$.

Gemäß unserer Vereinbarung enthält FP nicht nur nicht-negative Funktionen. In Punkt 1 beispielsweise hätten wir also äquivalent auch schreiben können: $\text{Gap-P} = \#\,\mathrm{P} + \mathrm{FP}$. Wir ziehen jedoch die obige Schreibweise vor, weil sie suggestiver ist und deutlich macht, daß an dieser Stelle negative Werte entscheidend sind. Im Verlauf der Arbeit werden wir auch immer wieder – aus genau diesem Grund – die Schreibweise $-\mathrm{FP}$ verwenden.

Weiterhin führen wir drei Operatoren ein, die angewendet auf Funktionenklassen als Resultat Mengenklassen ergeben. Ihre Definition ist implizit vorhanden in der Definition der Klassen UP [Val76], XP [OgHe93] und $\oplus\,\mathrm{P}$ [PaZa83] (die zweite dieser Klassen ist auch unter dem Namen SPP bekannt [FeFoKu91]).

Sei dazu $\mathcal{F}$ eine Klasse von Funktionen. Dann definieren wir die Klasse $\mathrm{U} \cdot \mathcal{F}$ als die Klasse aller Mengen, deren charakteristische Funktion zu $\mathcal{F}$ gehört und die Klasse $\mathrm{X} \cdot \mathcal{F}$ als die Klasse aller Mengen, deren charakteristische Funktion zu $\mathcal{F} - \mathcal{F}$ gehört. $\oplus \cdot \mathcal{F}$ besteht aus denjenigen Mengen A, für die ein $f \in \mathcal{F}$ existiert, so daß $x \in A$ gdw. $f(x)$ ungerade ist. Offensichtlich ist $\mathrm{UP} = \mathrm{U} \cdot \#\,\mathrm{P}$, $\mathrm{XP} = \mathrm{X} \cdot \#\,\mathrm{P} = \mathrm{U} \cdot \text{Gap-P} = \mathrm{X} \cdot \text{Gap-P}$ und $\oplus\,\mathrm{P} = \oplus \cdot \#\,\mathrm{P}$. Weiterhin ist bekannt [KöScTo89, Sparta91], daß $\mathrm{U}(\text{span-P} - \mathrm{FP}) = \mathrm{X}(\text{span-P} - \mathrm{FP}) = \mathrm{XP}^{\mathrm{NP}}$. Für eine Mengenklasse $\mathcal{K}$ verwenden wir die abkürzenden Schreibweisen $\mathrm{U}\mathcal{K}$, $\mathrm{X}\mathcal{K}$ und $\oplus\,\mathcal{K}$ für $\mathrm{U}\,\#\,\mathcal{K}$, $\mathrm{X}\,\#\,\mathcal{K}$ und $\oplus\,\#\,\mathcal{K}$.

3 Medianfunktionen

Seinosuke Toda definierte im Jahre 1990 in seiner Arbeit [Tod90] die Klasse Mid P.

3.1 Definition. Die Klasse Mid P besteht aus genau den Funktionen h, für die eine nichtdeterministische polynomiell-zeitbeschränkte Turingmaschine M mit Ausgabe existiert, so daß folgendes gilt: Ist die Menge aller Ausgabewerte von M bei Eingabe x die Menge

$$\{z_0, z_1, \ldots, z_k\}, \quad z_0 < z_1 < \cdots < z_k,$$

so ist $h(x) =_{\mathrm{def}} z_{\lfloor k/2 \rfloor}$. Wir sagen abkürzend, daß M die Funktion h berechnet.

Toda führte diese Klasse ein mit dem Ziel, eine einfache Charakterisierung der Klasse $\mathrm{FP}^{\#\mathrm{P}}$ zu finden und natürliche vollständige Probleme für jene Klasse angeben zu können. Er zeigte, daß $\mathrm{FP}^{\#\mathrm{P}}$ aus genau den Funktionen besteht, die von einer FP-Maschine mit nur einer Frage an eine Orakelfunktion aus Mid P berechnet werden können, und folgerte daraus, daß eine Reihe von funktionalen Problemen, die durch einen Medianbildungs-Prozeß aus NP-vollständigen Entscheidungsproblemen entstehen, für $\mathrm{FP}^{\#\mathrm{P}}$ vollständig sind unter metrischen Reduktionen [Kre88].

Wir untersuchen in diesem Kapitel eine Klasse von Funktionen, die sich nur in einem subtilen Punkt von Todas Klasse Mid P unterscheidet. Ausgangspunkt sind erneut nichtdeterministische Polynomialzeit-Maschinen mit Ausgabe, aber wir bilden nicht zunächst die *Menge* aller Ausgabewerte, um dann daraus den Median zu bestimmen, sondern wir betrachten direkt die *Folge* der Ausgabewerte der Maschine und nehmen sie als Ausgangspunkt für die Medianbildung; d. h. also daß bei uns Werte, die mehr als einmal ausgegeben werden, auch mit ihren tatsächlichen Vielfachheiten berücksichtigt werden.

3.2 Definition. Die Klasse Med P besteht aus genau den Funktionen h, für die eine nichtdeterministische polynomiell-zeitbeschränkte Turingmaschine mit

Ausgabe existiert, so daß folgendes gilt: Ist die geordnete Folge aller Ausgabewerte von M bei Eingabe x (mit Vielfachheiten) die Folge

$$z_0 \leq z_1 \leq \cdots \leq z_{g(x)},$$

so ist $h(x) =_{\mathrm{def}} z_{\lfloor g(x)/2 \rfloor}$.

Wir zeigen, daß auch die Klasse Med P eine Charakterisierung von $\mathrm{FP}^{\#\mathrm{P}}$ erlaubt, die der von Toda gefundenen sehr verwandt ist. Dies mag auf den ersten Blick nicht sonderlich überraschen, wirkt doch der Unterschied in der Definition der Klassen zunächst nur geringfügig. Wir werden jedoch anschließend zeigen, daß beide Klassen tatsächlich sehr unterschiedliche Eigenschaften aufweisen. Wir werden die Klassen in ein Inklusionsdiagramm zusammen mit den Klassen FP, # P, Gap-P und span-P einordnen (siehe Bild 3.1) und sodann zeigen, daß unter allgemein-vermuteten komplexitätstheoretischen Annahmen alle Inklusionen dieses Diagramms echt sind, was zeigt, daß Mid P und Med P (vermutlich) verschiedene Klassen sind. Bei der Erzielung dieses Resultats zeigt sich die Eleganz der modernen operatorentheoretischen Sichtweise der strukturellen Komplexitätstheorie. Um von zwei Klassen zu demonstrieren, daß sie nicht zusammenfallen, wählen wir einen der in Kapitel 2 eingeführten Operatoren, der so beschaffen ist, daß er die feinen Unterschiede zwischen den Klassen deutlich macht, indem er sie in Mengenklassen überführt, die deutlich unterschiedliche Eigenschaften aufweisen.

Die Vermutung der Verschiedenheit der beiden Medianklassen wird weiterhin gestützt durch die Vollständigkeitsresultate, die wir in den letzten beiden Abschnitten dieses Kapitels beweisen werden. Es zeigt sich nämlich, daß die Klassen unter einem strengen von uns hier eingeführten Reduktionsbegriff zwischen Funktionen durch verschiedene vollständige Probleme charakterisiert werden; und zwar handelt es sich bei diesen Problemen um Variationen jener, von denen Toda in [Tod90] bewies, daß sie vollständig sind für $\mathrm{FP}^{\#\mathrm{P}}$ unter einem „lockeren“ Reduktionsbegriff, der die Feinheiten der Unterschiede zwischen den Klassen verwischt.

3.1. Inklusionsbeziehungen zwischen den Funktionenklassen

3.1.1. Ein mengentheoretischer Medianoperator

Der Unterschied in der Definition der Klassen Mid P und Med P liegt also darin, daß im ersten Fall Vielfachheiten nicht berücksichtigt werden und im zweiten Fall berücksichtigt werden. Es zeigt sich, daß es günstig ist, zum Vergleich der Klassen eine weitere Mediansklasse einzuführen, bei der per definitionem die Frage nach Vielfachheiten nicht entsteht.

3.3 Definition. Die Funktionenklasse $\mathrm{M\overline{ed}}\,\mathcal{K}$ für eine Klasse $\mathcal{K}$ von Mengen besteht aus genau den Funktionen h, für die ein $A \in \mathcal{K}$, sowie Funktionen $g_1, g_2 \in \mathrm{FP}$, $g_1 < g_2$, existieren, derart daß $h(x)$ gleich dem mittleren Element der Menge

$$\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in A \,\}$$

ist; d. h. also ist die obige Menge gleich $\{z_0, z_1, \ldots, z_k\}$, $z_0 < z_1 < \cdots < z_k$, so ist $h(x) =_{\mathrm{def}} z_{\lfloor k/2 \rfloor}$.

Da wir in dieser Definition von Mengenklassen ausgehen und da eine Menge ein Element entweder enthält oder nicht enthält (aber nicht zweimal, dreimal, ... enthält), sind die Auftreten von zu berücksichtigenden Elementen hier eindeutig. Das erlaubt es uns zu zeigen:

3.4 Beobachtung. $\mathrm{M\overline{ed}}\,\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P} \cap \mathrm{Mid}\,\mathrm{P}$.

Beweis. Sei $f \in \mathrm{M\overline{ed}}\,\mathrm{P}$ folgendermaßen definiert: $f(x)$ ist das mittlere Element der Menge $\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in A \,\}$ für ein $A \in \mathrm{P}$ und Funktionen $g_1, g_2 \in \mathrm{FP}$.

Man betrachte die Turingmaschine M, die gegeben x zunächst ein y aus dem Bereich $g_1(x) \leq y \leq g_2(x)$ rät. Sodann überprüft M, ob $(x,y) \in A$; falls ja, gibt sie y aus; andernfalls verzweigt sie sich auf zwei verschiedene Pfade und gibt auf einem der beiden den Wert $g_1(x) - 1$ und auf dem anderen den Wert $g_2(x) + 1$ aus.

Auf diese Art und Weise wird sichergestellt, daß jedes y, $g_1(x) \leq y \leq g_2(x)$, mit $(x,y) \in A$ als Ausgabewert von M vorkommt und in die Medianbildung einfließt. Werte y aus dem relevanten Bereich mit $(x,y) \notin A$ führen zu einer Ausgabe von zwei Werten, die insgesamt die Medianbildung nicht beeinflussen. □

Es zeigt sich, daß das obige Resultat in einer Richtung sogar verstärkt werden kann. Mit Hilfe des Operators $\mathrm{M\overline{ed}}$ kann nämlich folgende alternative Charakterisierung von Todas Klasse $\mathrm{Mid}\,\mathrm{P}$ angegeben werden.

3.5 Satz. $\mathrm{Mid}\,\mathrm{P} = \mathrm{M\overline{ed}}\,\mathrm{NP}$.

Beweis. $\supseteq$: Es sei $f \in \mathrm{M\overline{ed}}\,\mathrm{NP}$, $f(x) = \mathrm{med}\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in A \,\}$, für eine Menge $A \in \mathrm{NP}$ und Funktionen $g_1, g_2 \in \mathrm{FP}$. Die Menge A werde erkannt von der Turingmaschine M. Man betrachte die folgendermaßen definierte Maschine M':

> Bei Eingabe x verzweigt M' zunächst für alle Paare (y,p), wobei $g_1(x) \leq y \leq g_2(x)$ und p Kodierung eines Pfades von M ist. Akzeptiert nun M die Eingabe (x,y) auf Pfad p, so gibt M' den Wert y aus; ansonsten gibt M' die Werte $g_1(x) - 1$ und $g_2(x) + 1$ aus.

Jeder Wert y mit $g_1(x) \leq y \leq g_2(x)$, der bei der Medianbildung bei f berücksichtigt wird, wird von M' ausgegeben, eventuell mehrere Male, aber die Vielfachheiten werden bei $\mathrm{Mid}\,\mathrm{P}$ nicht berücksichtigt. Alle anderen Werte y führen zu einer irrelevanten Ausgabe von M'.

Also ist $f(x)$ das mittlere Element in der Menge der Ausgaben von M' bei Eingabe x. Damit ist $f \in \mathrm{Mid}\,\mathrm{P}$.

$\subseteq$: Es werde $f \in \mathrm{Mid}\,\mathrm{P}$ berechnet von der Maschine M. Wähle $g_1, g_2 \in \mathrm{FP}$ so, daß $g_1(x) \leq f(x) \leq g_2(x)$ für alle x. Betrachte die Menge

$$\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge \text{es existiert ein Pfad von } M \text{ bei Eingabe } x, \\ \text{auf dem } y \text{ ausgegeben wird} \,\}.$$

Diese Menge ist offensichtlich in NP und gleich der Menge der Ausgaben von M bei Eingabe x. Das mittlere Element der Menge ist also gleich $f(x)$. Damit ist $f \in \mathrm{M\overline{ed}}\,\mathrm{NP}$. □

Aufgrund der einfachen Beobachtung, daß 3.4 relativiert werden kann, ergibt sich direkt folgendes Korollar:

3.6 Korollar. $\mathrm{Mid}\,\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P}^{\mathrm{NP}}$.

3.1.2. Medianbestimmungen simulieren Zählprozesse

Toda zeigte, daß $\mathrm{Mid}\,\mathrm{P}$ und $\#\,\mathrm{P}$ in gewissen Kontexten gleiche Komplexität haben. Das genaue Verhältnis der Klassen zueinander blieb in [Tod90] jedoch offen. In diesem Abschnitt geben wir Simulationen der Zählprozesse, die zu den Klassen Gap-P und span-P − FP führen, durch verschiedene Medianbildungs-Prozesse an. Es zeigt sich, daß Gap-P eine Teilklasse von $\mathrm{M\overline{ed}}\,\mathrm{P}$ (und damit auch von den anderen betrachteten Medianklassen) ist; span-P − FP, eine Oberklasse von Gap-P, scheint jedoch erst in $\mathrm{M\overline{ed}}\,\mathrm{NP} = \mathrm{Mid}\,\mathrm{P}$ enthalten zu sein. Wir werden im Abschnitt 3.2 sehen, daß dieses Ergebnis auch nicht verbessert werden kann, d. h. unter vernünftigen komplexitätstheoretischen Annahmen ist span-P − FP nicht in $\mathrm{Med}\,\mathrm{P}$ enthalten.

3.7 Satz.

1. $\#\,\mathrm{P} \subseteq \mathrm{M\overline{ed}}\,\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P}$.

2. $\text{span-P} = \#\,\mathrm{NP} \subseteq \mathrm{Mid\,P}$.

Beweis.

1. Es sei $B \in \mathrm{P}$, $g \in \mathrm{FP}$ und $f \in \#\,\mathrm{P}$ definiert als
$$f(x) = |\{\, y \mid 0 \leq y \leq g(x) \wedge (x, y) \in B \,\}|\,.$$
Definiere
$$\begin{aligned} D =_{\text{def}} & \{\,(x, y) \mid -g(x) \leq y \leq g(x)\,\} \\ & \cup \{\,(x, g(x) + 2y + 1) \mid 0 \leq y \leq g(x) \wedge (x, y) \in B\,\} \\ & \cup \{\,(x, g(x) + 2y + 2) \mid 0 \leq y \leq g(x) \wedge (x, y) \in B\,\} \end{aligned}$$
Sicherlich ist dann $D \in \mathrm{P}$. Der Median über alle y aus $\{\,(x, y) \mid -g(x) \leq y \leq g(x)\,\}$ ist klarerweise 0. Für jeden Wert y, $0 \leq y \leq g(x)$, für den $(x, y) \in B$, wird ein Tupel in die Teilmenge von D aus der zweiten Zeile und ein Tupel in die Teilmenge von D aus der dritten Zeile aufgenommen. Der Median vergrößert sich also für jedes solche y um den Wert 1. Damit ist das „mittlere y" mit $(x, y) \in D$ gleich $|\{\, y \mid 0 \leq y \leq g(x) \wedge (x, y) \in B \,\}|$.

2. Wähle in Punkt 1 $B \in \mathrm{NP}$, dann ist auch $D \in \mathrm{NP}$. Daraus ergibt sich $\#\,\mathrm{NP} \subseteq \mathrm{M\overline{ed}\,NP}$. Behauptung 2 folgt dann aus Satz 3.5.

□

Es ergibt sich direkt folgendes Korollar:

3.8 Korollar.

1. $\text{Gap-P} \subseteq \mathrm{M\overline{ed}\,P} \subseteq \mathrm{Med\,P}$.

2. $\text{span-P} - \mathrm{FP} \subseteq \mathrm{Mid\,P}$.

Beweis. Eine einfache Beobachtung zeigt, daß die betrachteten Medianklassen abgeschlossen sind unter Subtraktion von FP-Funktionen. Man lasse beispielsweise eine Maschine, die eine Mid P-Funktion berechnet, anstelle ihres eigentlichen Ausgabewertes den um den Wert einer FP-Funktion verminderten Wert ausgeben. □

Satz 3.7 läßt sich verallgemeinern auf andere Stufen der Hierarchie der Zählfunktionen:

3.9 Korollar. $k\,\#\,\mathrm{P} \subseteq \mathrm{M\overline{ed}\,P}^{\left.\mathrm{M\overline{ed}\,P}^{\cdot^{\cdot^{\cdot^{\mathrm{M\overline{ed}\,P}}}}}\right\}k\ \text{mal}}$.

Beweis. Satz 3.7 ist relativierbar. Die Behauptung folgt dann aus einer trivialen Induktion.

□

3.1.3. Charakterisierungen der Klasse $\mathrm{FP}^{\#\mathrm{P}}$

Todas Ziel bei der Einführung seiner Medianklasse war eine Charakterisierung der Klasse $\mathrm{FP}^{\#\mathrm{P}}$, die er mit folgendem Resultat angab:

3.10 Satz. $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\mathrm{Mid\,P}} = \mathrm{FP}^{\mathrm{Mid\,P}}[1]$.

In diesem Abschnitt werden wir zeigen, daß wir in diesem Satz Mid P durch eine der anderen Medianklassen ersetzen können. Weiterhin werden wir sehen, daß die gleiche Klasse ebenfalls charakterisiert werden kann als Klasse der Funktionen, die sich als Differenz zweier Mid P-, Med P- oder $\overline{\mathrm{Med}}$ P-Funktionen schreiben lassen.

3.11 Satz. $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\overline{\mathrm{Med}}\,\mathrm{P}} = \mathrm{FP}^{\overline{\mathrm{Med}}\,\mathrm{P}}[1] = \overline{\mathrm{Med}}\,\mathrm{P} - \overline{\mathrm{Med}}\,\mathrm{P}$.

Beweis. $\overline{\mathrm{Med}}\,\mathrm{P} \subseteq \mathrm{Mid\,P}$, also folgt aus Todas Resultat direkt $\mathrm{FP}^{\overline{\mathrm{Med}}\,\mathrm{P}} \subseteq \mathrm{FP}^{\#\mathrm{P}}$. Für die andere Richtung zeigen wir zunächst $\mathrm{FP}^{\mathrm{PP}} \subseteq \mathrm{FP}^{\overline{\mathrm{Med}}\,\mathrm{P}}[1]$:

Es sei also $h \in \mathrm{FP}^{\mathrm{PP}}$. h werde berechnet von der deterministischen Orakel-Maschine M mit Fragen an das Orakel $A \in \mathrm{PP}$. A werde entschieden von der probabilistischen Maschine M'. M' verzweige sich auf eine Anzahl von Pfaden, die nur von der Eingabe x an M abhängt. Weiterhin sei diese Anzahl stets ungerade. Wähle $r \in \mathrm{Pol}$ so, daß für jede Eingabe x der Länge n die Maschine M genau $r(n)$ Fragen an A stellt. Wähle weiterhin $g \in \mathrm{FP}$ so, daß für jede Eingabe x der Länge n von M sowohl die Fragen von M als auch Kodierungen von Pfaden der Berechnung von M' bei Eingabe dieser Fragen aus der Menge $[g(x)]$ stammen.

Definiere nun die Menge B als Menge aller Paare

$$(x, \langle z, p_{r(|x|)}, y_{r(|x|)}, a_{r(|x|)}, \ldots, p_1, y_1, a_1\rangle_{g(x)}),$$

für die gilt:

1. $a_i \in \{0,1\}$ für $i = 1, \ldots, r(|x|)$.
2. Bei Eingabe x stellt die Maschine die Fragen $y_1, \ldots, y_{r(|x|)}$, falls sie für die Antworten die Werte $a_1, \ldots, a_{r(|x|)}$ annimmt.
3. Bei Eingabe x gibt die Maschine den Wert z aus, falls sie für die Antworten die Werte $a_1, \ldots, a_{r(|x|)}$ annimmt.
4. Für $i = 1, \ldots, r(|x|)$ gilt: Machine M' akzeptiert die Eingabe y_i auf Pfad p_i genau dann, wenn $a_i = 1$.

Mit Hilfe von B wird eine Rechnung der Maschine M bei Eingabe eines Wortes x folgendermaßen simuliert:

M rechnet zunächst deterministisch und produziert eine Frage z_1 an A. Wir starten sodann die Maschine M' und ordnen alle Pfade von M' bei Eingabe z_1 bezüglich Verwerfen/Akzeptieren. Klarerweise können wir auf dem mittleren Pfad dann die korrekte Antwort des Orakels ablesen. Fahren wir am Ende jedes Pfades mit der Simulation von M fort, wird also auf dem mittleren Pfad korrekt simuliert und eine Frage z_2 produziert. Erneut starten wir M', ordnen die Pfade und fahren auf dem mittleren Pfad mit der korrekten Simulation fort. Da die Anzahl der Fragen polynomiell ist, läßt sich die ganze Prozedur in Polynomialzeit durchführen.

Dem mittleren

$$y = \langle z, p_{r(|x|)}, y_{r(|x|)}, a_{r(|x|)}, \ldots, p_1, y_1, a_1 \rangle_{g(x)}$$

mit $(x, y) \in B$ können wir also das Ergebnis der Simulation ablesen. Damit ist also $\mathrm{FP}^{\mathrm{PP}} \subseteq \mathrm{FP}^{\mathrm{M\overline{ed}\,P}}[1]$.

Definieren wir nun B' analog zu B mit dem einzigen Unterschied, daß nun in den definierenden Bedingungen der Punkt 3 durch $z = 0$ ersetzt wird, so zeigt sich, daß, wenn wir das mittlere y' mit $(x, y') \in B'$ von dem mittleren y wie oben subtrahieren, wir genau den Wert $h(x)$ erhalten. Damit ist also $\mathrm{FP}^{\mathrm{PP}} \subseteq \mathrm{M\overline{ed}\,P} - \mathrm{M\overline{ed}\,P}$. □

Es ergeben sich folgende Korollare:

3.12 Korollar. $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{FP}^{\mathrm{Med\,P}} = \mathrm{FP}^{\mathrm{Med\,P}}[1] = \mathrm{Med\,P} - \mathrm{Med\,P}$.

Beweis. $\mathrm{Med\,P} \subseteq \mathrm{FP}^{\mathrm{PP}}$ zeigt eine einfache binäre Suche mittels Fragen an eine geeignete $\#\,\mathrm{P}$-Funktion. Alle anderen Inklusionen sind direkte Konsequenzen aus 3.11 und 3.4. □

Die Aussage von Todas Satz 3.10 kann erweitert werden um die Klasse der Differenzen von zwei Mid P-Funktionen:

3.13 Korollar. $\mathrm{FP}^{\#\mathrm{P}} = \mathrm{Mid\,P} - \mathrm{Mid\,P}$.

Für die Hierarchie der Zählfunktionen ergibt sich:

3.14 Korollar.

$$\mathrm{FP}^{k\#\mathrm{P}} = \mathrm{FP}^{\left.\mathrm{M\overline{ed}\,P}^{\mathrm{M\overline{ed}\,P}^{\cdot^{\cdot^{\mathrm{M\overline{ed}\,P}}}}}\right\} k \text{ mal}}[1].$$

Beweis. Die obigen Sätze und Korollare sind relativierbar. Insbesondere implizieren sie $\#\,\mathrm{P}^{\mathrm{M\overline{ed}\,P}} = \#\,\mathrm{P}^{\mathrm{Med\,P}} = \#\,\mathrm{P}^{\mathrm{Mid\,P}} = \#\,\mathrm{P}^{\#\mathrm{P}}$. Der Beweis ist nun eine einfache Induktion. □

Natürlich kann auch eine Analogon zu Korollar 3.14 mit den Klassen Med P und Mid P angegeben werden.

3.2. Transformationen in Mengenklassen

Abbildung 3.1 faßt unsere bisherigen Ergebnisse zusammen. $\mathrm{Med\,P}^{\mathrm{NP}} \subseteq \mathrm{P}^{\mathrm{PP}}$ folgt aus einer Relativierung von $\mathrm{Med\,P} \subseteq \mathrm{P}^{\mathrm{PP}}$ und der Beziehung $\#\mathrm{PH} \subseteq \mathrm{FP}^{\#\mathrm{P}}[1]$ aus [ToWa91], die $\mathrm{P}^{\mathrm{PP}} = \mathrm{P}^{\mathrm{PP}^{\mathrm{NP}}}$ impliziert. Die Abbildung zeigt unterschiedliche Positionen für die verschiedenen Medianklassen; dennoch haben wir bisher keine Evidenz dafür, daß die betrachteten Medianklassen nicht zusammenfallen. Das möchten wir in diesem Abschnitt tun.

Wir stützen uns auf folgende operatorentheoretische Herangehensweise: Es seien $\mathcal{F}_1$ und $\mathcal{F}_2$ Funktionenklassen, für deren Verschiedenheit wir Gründe angeben möchten. Dann wählen wir einen Operator $\mathcal{O}$, der die Unterschied zwischen $\mathcal{F}_1$ und $\mathcal{F}_2$ derart deutlich macht, daß er sie in Mengenklassen $\mathcal{K}_1 = \mathcal{O} \cdot \mathcal{F}_1$ und $\mathcal{K}_2 = \mathcal{O} \cdot \mathcal{F}_2$ überführt, deren Verschiedenheit allgemein akzeptiert ist. Gibt es zum Beispiel eine komplexitätstheoretische Hypothese Ξ, deren Gültigkeit $\mathcal{K}_1 \neq \mathcal{K}_2$ impliziert, also $\Xi \models \mathcal{K}_1 \neq \mathcal{K}_2$, dann gilt natürlich auch $\Xi \models \mathcal{F}_1 \neq \mathcal{F}_2$. Sind die betrachteten Klassen relativierbar und gibt es ein Orakel O, das $\mathcal{K}_1$ von $\mathcal{K}_2$ trennt, so trennt es auch $\mathcal{F}_1$ von $\mathcal{F}_2$.

Wir beginnen, indem wir einen Operator einführen, der auch in den kommenden Kapiteln eine sehr große Rolle spielen wird:

3.15 Definition. Es sei $\mathcal{F}$ eine Klasse von Funktionen. Dann definiern wir die Klasse $\mathrm{S} \cdot \mathcal{F}$ als die Klasse aller Mengen A, für die Funktionen $f \in \mathcal{F}$ und $g \in \mathrm{FP}$ existieren, so daß gilt: $x \in A \iff f(x) \geq g(x)$.

Der Operator S ist eng verwandt mit dem mengentheoretischen Zählquantor C. Für jede Mengenklasse $\mathcal{K}$ ergibt C angewandt auf $\mathcal{K}$ genau das Ergebnis von S angewandt auf die Klasse $\#\mathcal{K}$.

Wir wenden nun S an auf die Funktionenklassen von Abbildung 3.1.

3.16 Satz.

1. $\mathrm{S} \cdot \mathrm{FP}^X = \mathrm{P}^X$ *für jede Klasse von Mengen oder Funktionen* X.
2. $\mathrm{S} \cdot \#\mathrm{P} = \mathrm{S} \cdot \text{Gap-P} = \mathrm{S} \cdot \mathrm{M\overline{ed}\,P} = \mathrm{S} \cdot \mathrm{Med\,P} = \mathrm{PP}$.
3. $\mathrm{S} \cdot \text{span-P} = \mathrm{S} \cdot \mathrm{Mid\,P} = \mathrm{S} \cdot \mathrm{Med\,P}^{\mathrm{NP}} = \mathrm{PP}^{\mathrm{NP}}$.

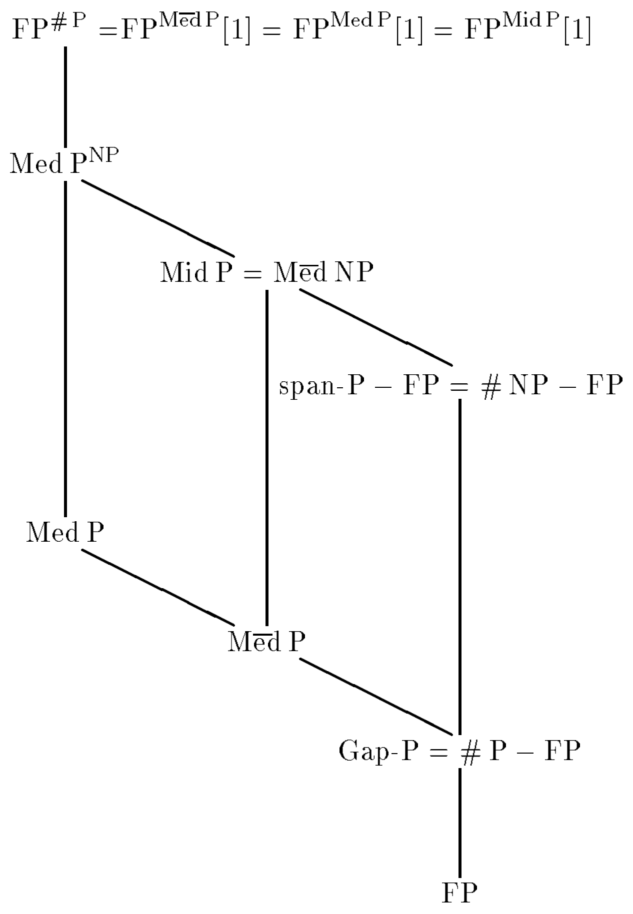

Abbildung 3.1: Inklusionsbeziehungen zwischen den betrachteten Klassen

Beweis.

1. Trivial.

2. $\mathrm{PP} \subseteq \mathrm{S} \cdot \#\mathrm{P}$ ergibt sich aus der obigen Bemerkung. Da die Funktionenklassen aus der zweiten Zeile von links nach rechts aufsteigend eine Inklusionskette bilden und da der Operator S offensichtlich monoton ist, reicht es, $\mathrm{S} \cdot \mathrm{Med}\,\mathrm{P} \subseteq \mathrm{PP}$ zu beweisen.

   Sei dazu $A \in \mathrm{S} \cdot \mathrm{Med}\,\mathrm{P}$; $x \in A \iff f(x) \geq g(x)$ für $f \in \mathrm{Med}\,\mathrm{P}$ und $g \in \mathrm{FP}$. M sei die Maschine, die f berechnet. Betrachte nun folgende Funktionen:

   $$\begin{aligned} \mathrm{G}(x) &= |\{\, z \mid \text{auf Pfad } z \text{ gibt } M \text{ bei Eingabe } x \text{ einen Wert} \geq g(x) \text{ aus}\,\}| \\ \mathrm{K}(x) &= |\{\, z \mid \text{auf Pfad } z \text{ gibt } M \text{ bei Eingabe } x \text{ einen Wert} < g(x) \text{ aus}\,\}| \end{aligned}$$

   Die Bedingung in der Klammer kann in Polynomialzeit überprüft werden. Also sind $\mathrm{G}, \mathrm{K} \in \#\mathrm{P}$. Eine Eingabe x gehört dann zu A, wenn der Median größer als $g(x)$ ist, also genau dann, wenn die Anzahl der Elemente $\geq g(x)$ größer der Anzahl der Elemente $< g(x)$ ist, d. h. $x \in A \iff \mathrm{G}(x) > \mathrm{K}(x) \iff \mathrm{G}(x) - \mathrm{K}(x) > 0$. Fenner, Fortnow und Kurtz [FeFoKu91] zeigten, daß durch Bedingungen dieser Form genau die Mengen in PP definiert werden. Damit ergibt sich also $A \in \mathrm{PP}$.

3. Aus einer Relativierung des obigen Beweises folgern wir $\mathrm{S} \cdot \mathrm{Med}\,\mathrm{P}^{\mathrm{NP}} \subseteq \mathrm{PP}^{\mathrm{NP}}$. Wagner [Wag86a] zeigte $\mathrm{PP}^{\mathrm{NP}} \subseteq \mathrm{S} \cdot \#\,\mathrm{NP}$. Die Behauptung ergibt sich nun wiederum daraus, die die Funktionenklassen von links nach rechts aufsteigend eine Inklusionskette bilden.

$\square$

Damit ergeben sich folgende Konsequenzen:

3.17 Korollar.

1. *Falls* $\mathrm{Med}\,\mathrm{P}^{\mathrm{NP}} = \mathrm{FP}^{\#\mathrm{P}}$, *dann ist* $\mathrm{PP}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{PP}}$.

2. *Falls* $\text{span-P} - \mathrm{FP} \subseteq \mathrm{Med}\,\mathrm{P}$, *dann ist* $\mathrm{PP} = \mathrm{PP}^{\mathrm{NP}}$.

Aus der Konsequenz der ersten Zeile ergibt sich, daß die Inklusionskette $\mathrm{PP}^{\mathrm{NP}} \subseteq \mathrm{PP}^{\mathrm{PH}} \subseteq \mathrm{MidBitP} \subseteq \mathrm{P}^{\mathrm{PP}}$ auf $\mathrm{PP}^{\mathrm{NP}}$ kollabiert und damit die Klasse MidBitP [GKRTT92, KöTo93] eine Reihe von unwahrscheinlichen Abschlußeigenschaften besitzt, ja sogar unter Turing-Reduktionen abgeschlossen ist. Darüberhinaus [Gre90] existiert ein Orakel, das $\mathrm{PP}^{\mathrm{PH}}$ von P^{PP} trennt. Aus der Konsequenz

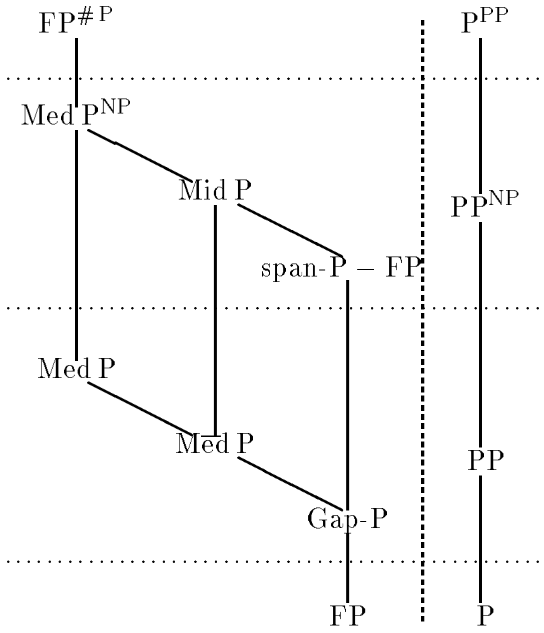

Abbildung 3.2: Transformationen unter S

der zweiten Zeile ergibt sich, daß $\Sigma_2^p \subseteq \mathrm{PP}$; was zumindest in gewissen relativierten Welten nicht gilt [Bei92]. Für jede vertikale Inklusion aus Abbildung 3.1 existiert also ein Orakel, daß sie echt macht. Abbildung 3.2 faßt die Transformationen von Satz 3.16 noch einmal zusammen.

Es bleibt also noch, die Klassen auf den Diagonalen voneinander zu trennen. Dazu untersuchen wir ihre Bilder unter den Operatoren U und X.

3.18 Satz.

1. $\mathrm{U} \cdot \mathrm{M\overline{ed}\,P} = \mathrm{XP}$.

2. $\mathrm{U} \cdot \mathrm{Med\,P} = \mathrm{PP}$.

Beweis.

1. Aufgrund von Korollar 3.8 gilt $\mathrm{XP} = \mathrm{U} \cdot \text{Gap-P} \subseteq \mathrm{U} \cdot \mathrm{M\overline{ed}\,P}$. Zu zeigen bleibt also noch $\mathrm{U} \cdot \mathrm{M\overline{ed}\,P} \subseteq \mathrm{XP}$.

   Sei $A \in \mathrm{U} \cdot \mathrm{M\overline{ed}\,P}$ gegeben. Dann gibt es eine Menge $B \in \mathrm{P}$ und Funktionen $g_1, g_2 \in \mathrm{FP}$ derart, daß $c_A(x) = \mathrm{med}\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x, y) \in$

$B\,\}$. Man betrachte folgende Funktionen:

$$\begin{aligned} h_1(x) &= |\{\, y \mid g_1(x) \leq y \leq 0 \wedge (x,y) \in B \,\}| \\ h_2(x) &= |\{\, y \mid 1 \leq y \leq g_2(x) \wedge (x,y) \in B \,\}| \end{aligned}$$

Da $B \in \mathrm{P}$, sind sicherlich $h_1, h_2 \in \#\,\mathrm{P}$ und damit $h_2 - h_1 + 1 \in \text{Gap-P}$. Ist jedoch $x \in A$, so ist der Median der Menge

$$M =_{\text{def}} \{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in B \,\}$$

gleich 1, also gilt bei $|M|$ ungerade die Gleichung $h_2(x) = h_1(x) + 1$ und bei $|M|$ gerade $h_2(x) = h_1(x) + 2$, also $h_2(x) - h_1(x) + 1 \in \{2,3\}$; und falls $x \notin A$ ergibt sich analog $h_2(x) \in \{h_1(x) - 1, h_1(x)\}$, also $h_2(x) - h_1(x) + 1 \in \{0,1\}$. Fenner, Fortnow und Kurtz [FeFoKu91] zeigten, daß so definierte Mengen in XP liegen.

2. Für alle Klassen von Funktionen $\mathcal{F}$ ist $\mathrm{U}\mathcal{F} \subseteq \mathrm{S}\mathcal{F}$, also folgt aus 3.16, daß $\mathrm{U\,Med\,P} \subseteq \mathrm{PP}$. Aus der Definition von PP ergibt sich jedoch direkt die umgekehrte Inklusion.

□

3.19 Korollar.

1. $\mathrm{U} \cdot \mathrm{Mid\,P} = \mathrm{XP}^{\mathrm{NP}}$.

2. $\mathrm{U} \cdot \mathrm{Med\,P}^{\mathrm{NP}} = \mathrm{PP}^{\mathrm{NP}}$.

Beweis.

1. Aufgrund von 3.8 ergibt sich

$$\mathrm{XP}^{\mathrm{NP}} = \mathrm{X} \cdot \#\,\mathrm{NP} = \mathrm{U}(\#\,\mathrm{NP} - \mathrm{FP}) \subseteq \mathrm{U} \cdot \mathrm{Mid\,P}.$$

Eine Relativierung von Satz 3.18 ergibt $\mathrm{U.\,Mid\,P} \subseteq \mathrm{U} \cdot \mathrm{M\overline{ed}\,P}^{\mathrm{NP}} \subseteq \mathrm{XP}^{\mathrm{NP}}$.

2. Direkte Relativierung der zweiten Aussage von Korollar 3.18.

□

(Die Aussagen von Satz 3.18 und Korollar 3.19 werden zusammen mit bekannten, in Kapitel 2 zitierten Resultaten über Gap-P und span-P in Abbildung 3.3 bildlich dargestellt.)

3.20 Satz.

$$\mathrm{X} \cdot \mathrm{M\overline{ed}\,P} = \mathrm{X} \cdot \mathrm{Med\,P} = \mathrm{X} \cdot \mathrm{Mid\,P} = \mathrm{X} \cdot \mathrm{Med\,P}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{PP}}.$$

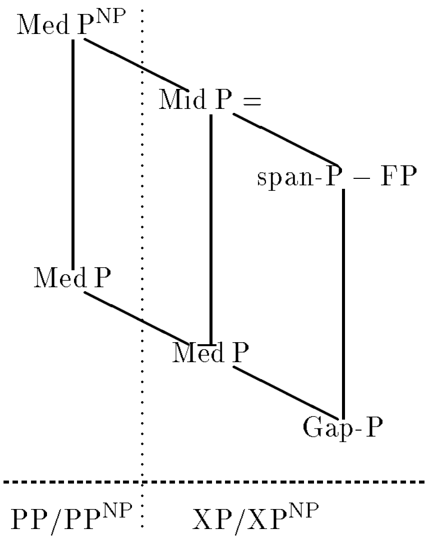

Abbildung 3.3: Transformationen unter U

Beweis. Trivialerweise gilt für jede Klasse von Mengen oder Funktionen X, daß $\mathrm{U} \cdot \mathrm{FP}^X = \mathrm{P}^X$. Nun folgt:

$$\begin{aligned} \mathrm{X} \cdot \mathrm{M\overline{ed}\,P} &= \mathrm{U} \cdot (\mathrm{M\overline{ed}\,P} - \mathrm{M\overline{ed}\,P}) && \text{(Definition von U und X)} \\ &= \mathrm{U} \cdot \mathrm{FP}^{\mathrm{PP}} && \text{(Satz 3.11)} \\ &= \mathrm{P}^{\mathrm{PP}} \end{aligned}$$

Die anderen Klassen liegen jedoch offensichtlich zwischen $\mathrm{X} \cdot \mathrm{M\overline{ed}\,P}$ und P^{PP}.

□

(Die Aussagen von Satz 3.20 werden zusammen mit bekannten, in Kapitel 2 zitierten Resultaten über Gap-P und span-P in Abbildung 3.4 bildlich dargestellt.)

Damit ergeben sich folgende Konsequenzen:

3.21 Korollar. *Die folgenden Aussagen sind äquivalent:*

1. $\mathrm{Gap\text{-}P} = \mathrm{M\overline{ed}\,P}$.

2. $\mathrm{M\overline{ed}\,P} = \mathrm{Med\,P}$.

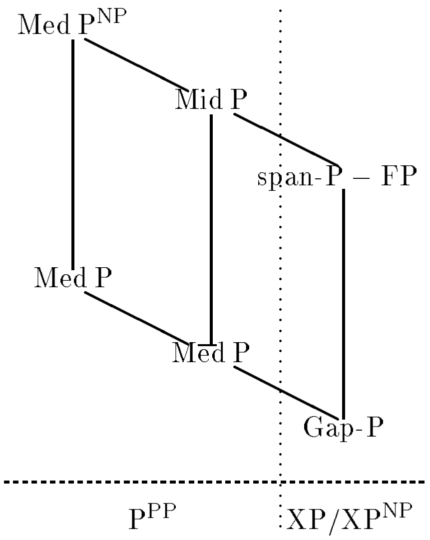

Abbildung 3.4: Transformationen unter X

3. *Die Counting-Hierarchie kollabiert auf* XP.

4. Gap-P = $\mathrm{FP}^{\mathrm{PP}}$.

Beweis. Falls Gap-P = $\mathrm{M}\overline{\mathrm{ed}}\,\mathrm{P}$, so folgt aus Satz 3.20 XP = P^{PP}, also insbesondere XP = PP. Falls $\mathrm{M}\overline{\mathrm{ed}}\,\mathrm{P}$ = Med P, so folgt aus Satz 3.18 XP = PP.

Fenner, Fortnow und Kurtz [FeFoKu91] zeigten, daß die Klasse XP low ist für PP und Gap-P. Aus XP = PP ergibt sich also sofort der Kollaps der Counting Hierarchie auf XP. Weiterhin folgt $\mathrm{FP}^{\mathrm{PP}} \subseteq \text{Gap-P}^{\mathrm{PP}} \subseteq \text{Gap-P}^{\mathrm{XP}} \subseteq \text{Gap-P} \subseteq$ Gap-P. Daraus folgen dann insbesondere wieder die ersten beiden Gleichheiten der Behauptung des Korollars. □

Aus der letzten Gleichheit der Behauptung von Korollar 3.21 folgt insbesondere, daß alle betrachteten Medianklassen zusammenfallen auf Gap-P. Die Bemerkung nach Korollar 3.17 zeigt also, daß wir Orakel haben, die die Klassen der unteren Diagonale in Abbildung 3.1 voneinander trennen.

3.22 Korollar. *Die folgenden Aussagen sind äquivalent:*

1. $\mathrm{M}\overline{\mathrm{ed}}\,\mathrm{P} \subseteq$ span-P − FP.

2. $\mathrm{Med\,P} \subseteq \mathrm{Mid\,P}$.

3. $\text{span-P} - \mathrm{FP} = \mathrm{Mid\,P}$.

4. $\mathrm{Mid\,P} = \mathrm{Med\,P}^{\mathrm{NP}}$.

5. Die Counting-Hierarchie kollabiert auf $\mathrm{XP}^{\mathrm{NP}}$.

6. $\mathrm{FP}^{\mathrm{PP}} = \text{span-P} - \mathrm{FP}$.

Beweis. Aus den obigen Resultaten ergibt sich:

- Falls $\mathrm{M\overline{ed}\,P} \subseteq \text{span-P} - \mathrm{FP}$, so gilt $\mathrm{P}^{\mathrm{PP}} = \mathrm{XP}^{\mathrm{NP}}$ (Satz 3.20).
- Falls $\mathrm{Med\,P} \subseteq \mathrm{Mid\,P}$, so gilt $\mathrm{PP} \subseteq \mathrm{XP}^{\mathrm{NP}}$ (Satz 3.18, Korollar 3.19).
- Falls $\text{span-P} - \mathrm{FP} = \mathrm{Mid\,P}$, so gilt $\mathrm{XP}^{\mathrm{NP}} = \mathrm{P}^{\mathrm{PP}}$ (Satz 3.20).
- Falls $\mathrm{Mid\,P} = \mathrm{Med\,P}^{\mathrm{NP}}$, so gilt $\mathrm{XP}^{\mathrm{NP}} = \mathrm{PP}^{\mathrm{NP}}$ (Korollar 3.19).

Aus allen vier Konsequenzen folgt direkt $\mathrm{PP} \subseteq \mathrm{XP}^{\mathrm{NP}}$. Daraus folgt jedoch (unter der Berücksichtigung der Tatsache , daß der Beweis der Lowness von XP für PP und Gap-P [FeFoKu91] relativierbar ist) $\mathrm{PP}^{\mathrm{PP}} \subseteq \mathrm{PP}^{\mathrm{XP}^{\mathrm{NP}}} \subseteq \mathrm{PP}^{\mathrm{NP}} \subseteq \mathrm{P}^{\mathrm{PP}}$. Diese Argumentation läßt sich induktiv fortsetzen zu $\mathrm{CH} = \mathrm{P}^{\mathrm{PP}}$. Daraus ergibt sich (wieder mit [FeFoKu91]) $\mathrm{FP}^{\mathrm{PP}} \subseteq \mathrm{FP}^{\mathrm{XP}^{\mathrm{NP}}} \subseteq \text{Gap-P}^{\mathrm{XP}^{\mathrm{NP}}} \subseteq \text{Gap-P}^{\mathrm{NP}} \subseteq \text{span-P} - \mathrm{FP}$. Daraus folgt nun die Gleichheit aller Klassen oberhalb $\text{span-P} - \mathrm{FP}$ aus Abbildung 3.1, also insbesondere die ersten vier Aussagen der Äquivalenzkette der Behauptung. Aufgrund von Punkt 1 kann nun $\mathrm{CH} = \mathrm{P}^{\mathrm{PP}}$ verschärft werden zu $\mathrm{CH} = \mathrm{XP}^{\mathrm{NP}}$. □

Man beachte, daß die oben erwähnten Orakelresultate [Gre90, Bei92] die Counting-Hierarchie von $\mathrm{XP}^{\mathrm{NP}}$ trennen. Damit existiert also für jede in Abbildung 3.1 angebene Inklusion ein Orakel, das sie strikt macht. Wir haben also gezeigt, daß unter allgemein akzeptierten komplexitätstheoretischen Annahmen alle Klassen aus Abbildung 3.1 verschieden voneinander sind. Jede Linie dieser Abbildung, die eine Inklusionsbeziehung angibt, wird in den Abbildungen 3.2, 3.3 oder 3.4 einmal von einer gestrichelten Linie gekreuzt.

3.3. Vollständigkeitsresultate für Funktionenklassen

Wir werden in diesem Abschnitt sehen, daß sich die verschiedenen Medianklassen als Abschluß gewisser natürlicher vollständiger funktionaler Probleme unter einem strengen Reduktionsbegriff ergeben. Zunächst wenden wir uns jedoch einer bekannteren funktionalen Reduzierbarkeit zu, nämlich metrischen Reduktionen.

3.3.1. Metrische Reduzierbarkeit

Mark Krentel führte in den achtziger Jahren folgenden Reduktionsbegriff zwischen Funktionen ein [Kre88]:

3.23 Definition. Die Funktion f ist genau dann metrisch reduzierbar auf die Funktion h ($f \leq_{met}^{\mathrm{FP}} h$), wenn zwei Funktionen $g, g' \in \mathrm{FP}$ existieren, so daß für alle x gilt: $f(x) = g'(x, h(g(x)))$.

Offensichtlich gelten folgende einfache Beobachtungen:

3.24 Beobachtung.

1. *Die Funktion f ist genau dann metrisch reduzierbar auf die Funktion h, wenn $f \in \mathrm{FP}^h[1]$.*
2. *Der Abschluß einer Funktionenklasse $\mathcal{F}$ unter metrischen Reduktionen ist gleich der Klasse $\mathrm{FP}^{\mathcal{F}}[1]$.*

Mit Hilfe dieser Beobachtungen zeigen nun die Resultate aus Abschnitt 3.1.3, daß metrische Reduktionen ungeeignet sind, um eine genaue Klassifizierung von Funktionen im Kontext der Medianklassen durchzuführen. Es gilt nämlich:

3.25 Korollar. *Der Abschluß jeder der Klassen $\mathrm{M\overline{e}d}\,\mathrm{P}$, $\mathrm{Med}\,\mathrm{P}$ und $\mathrm{Mid}\,\mathrm{P}$ unter metrischen Reduktionen ist gleich der Klasse $\mathrm{FP}^{\#\mathrm{P}}$.*

Beweis. Folgt direkt aus Beobachtung 3.24, Satz 3.11, Korollar 3.12 und Satz 3.10. □

3.26 Korollar. *Die Klassen $\mathrm{M\overline{e}d}\,\mathrm{P}$, $\mathrm{Med}\,\mathrm{P}$, $\mathrm{Mid}\,\mathrm{P}$ und $\mathrm{FP}^{\#\mathrm{P}}$ haben die gleichen harten Probleme bezüglich $\leq_{met}^{\mathrm{FP}}$.*

Toda bewies in [Tod90] von einer Reihe von natürlichen funktionalen Problemen, daß sie vollständig für $\mathrm{FP}^{\#\mathrm{P}}$ unter metrischen Reduktionen sind. Aus Korollar 3.26 folgt nun, daß diese Probleme hart für alle unsere Medianklassen sind. Wir werden uns im folgenden Todas Problemen (oder leichten Abwandlungen davon) zuwenden und sie unter einem strengeren Reduktionsbegriff genauer klassifizieren, indem wir ihre Vollständigkeit für verschiedene der Klassen aus Abbildung 3.1 beweisen.

3.3.2. Funktionale many-one-Reduzierbarkeit

Metrische Reduktionen laufen folgendermaßen ab: Ist $f \leq_{met}^{\mathrm{FP}} h$ vermöge der Funktionen $g, g' \in \mathrm{FP}$ und wollen wir den Wert $f(x)$ berechnen, so führen wir zunächst eine Transformation der Eingabe durch (indem wir $g(x)$ berechnen), werten die Funktion h an der Stelle der transformierten Eingabe aus (berechnen also $h(g'(x))$) und transformieren sodann das Ergebnis dieser Berechnung und erhalten so den Wert von f (also $f(x) = g'(x, h(g(x)))$).

Suchen wir einen strengeren Reduktionsbegriff, bietet es sich an, einfach auf die äußere Transformation zu verzichten und zu verlangen, daß das Ergebnis der Auswertung von h bereits der Wert $f(x)$ ist, an dem wir interessiert sind (siehe auch [Wag86b, S. 135] und [Köb89, Def. 1.5a]).

3.27 Definition. Die Funktion f ist genau dann funktional many-one-reduzierbar auf die Funktion h ($f \leq_m^{\mathrm{FP}} h$), wenn eine Funktion $g \in \mathrm{FP}$ existiert, so daß für alle x gilt: $f(x) = h(g(x))$.

Offensichtlich besitzt funktionale many-one-Reduzierbarkeit eine angenehme Eigenschaft, die sie bereits gegenüber der metrischen Reduzierbarkeit auszeichnet, daß nämlich die Funktionenklassen aus Abbildung 3.1 alle abgeschlossen sind unter $\leq_m^{\mathrm{FP}}$.

3.28 Lemma. *Die Klassen* Gap-P*,* span-P*,* $\mathrm{M\overline{ed}\,P}$*,* Med P*,* Mid P*,* $\mathrm{Med\,P^{NP}}$ *und* FP^X *(für eine beliebige Klasse von Mengen oder Funktionen X) sind abgeschlossen unter $\leq_m^{\mathrm{FP}}$.*

Beweis. Die Beweise sind offensichtlich. Sei beispielsweise M eine nichtdeterministische polynomiell-zeitbeschränkte Turingmaschine, die eine Funktion $f \in \mathrm{Med\,P}$ berechnet und sei $g \in \mathrm{FP}$, so wird $f \circ g$ berechnet von der Maschine M', die bei Eingabe x zunächst $g(x)$ berechnet und sodann die Arbeitsweise von M bei der Eingabe $g(x)$ simuliert. Alle anderen Beweise verlaufen vollkommen analog. □

3.29 Korollar.

1. *Ist eine Funktion, die hart ist für* Mid P *unter $\leq_m^{\mathrm{FP}}$, ein Element der Klasse* Med P*, so ist $\Sigma_2^p \subseteq \mathrm{PP}$.*

2. *Ist eine Funktion, die hart ist für* Med P *unter $\leq_m^{\mathrm{FP}}$, ein Element der Klasse* Mid P*, so kollabiert die Counting-Hierarchie auf* $\mathrm{P^{PP}}$.

Beweis. Aus Lemma 3.28 ergibt sich, daß aus den Annahmen im ersten Fall $\mathrm{Mid\,P} \subseteq \mathrm{Med\,P}$ und im zweiten Fall $\mathrm{Med\,P} \subseteq \mathrm{Mid\,P}$ folgt. Die angegebenen Konsequenzen ergeben sich dann aus den Bemerkungen nach Korollar 3.17 sowie aus Korollar 3.22. □

Es bleibt also zunächst einmal die Existenz von harten oder vollständigen Problemen für die Medianklassen unter $\leq_m^{\mathrm{FP}}$ zu untersuchen. Es lassen sich jedoch auf kanonische Weise künstliche universelle Funktionen für diese Klassen angeben. Dazu definieren wir (unter Voraussetzung der Existenz einer leicht zu berechnenden Kodierung von Turingmaschinen):

Problem:	$\mathrm{U{\scriptsize NIV}}_{\overline{\mathrm{Med}}\,\mathrm{P}}$
Gegeben:	die Kodierung einer deterministischen Turing-Maschine M, ein Wort x, eine Zahl j, eine Zahl k in unärer Darstellung
Gesucht:	das mittlere Element aller y mit $y \in [j]$, so daß (x, y) von der Maschine M in höchstens k Schritten akzeptiert wird

Problem:	$\mathrm{U{\scriptsize NIV}}_{\mathrm{Med}\,\mathrm{P}}$
Gegeben:	die Kodierung einer nichtdeterministischen Turing-Maschine M, ein Wort x, eine Zahl k (unär)
Gesucht:	das mittlere Element in der Folge aller Ausgabewerte der k-Schritte-Rechnung von M bei Eingabe x

Problem:	$\mathrm{U{\scriptsize NIV}}_{\mathrm{Mid}\,\mathrm{P}}$
Gegeben:	die Kodierung einer nichtdeterministischen Turing-Maschine M, ein Wort x, eine Zahl k (unär)
Gesucht:	das mittlere Element in der Menge aller Ausgabewerte der k-Schritte-Rechnung von M bei Eingabe x

3.30 Satz. *Für* $\mathcal{K} \in \{\overline{\mathrm{Med}}\,\mathrm{P}, \mathrm{Med}\,\mathrm{P}, \mathrm{Mid}\,\mathrm{P}\}$ *gilt:* $\mathrm{U{\scriptsize NIV}}_{\mathcal{K}}$ *ist vollständig für* $\mathcal{K}$ *unter* $\leq_m^{\mathrm{FP}}$.

Beweis. Die drei Beweise sind sehr ähnlich. Wir wählen den Fall $\mathcal{K} = \mathrm{Mid}\,\mathrm{P}$:

Es sei also $f \in \mathrm{Mid}\,\mathrm{P}$. f werde berechnet von der Turing-Maschine M. Sei $\langle M \rangle$ die Kodierung von M. Sei $p \in \mathrm{Pol}$ eine Schranke für die Laufzeit von M. Offensichtlich reduziert dann die folgende Funktion $g \in \mathrm{FP}$ die Funktion f auf $\mathrm{U{\scriptsize NIV}}_{\mathrm{Mid}\,\mathrm{P}}$:

$$g(x) =_{\mathrm{def}} (x, \langle M \rangle, 0^{p(|x|)}).$$

$\square$

Im Gegensatz zu Korollar 3.26 für metrische Reduktionen haben wir nun folgendes Resultat:

3.31 Korollar. *Haben die Klassen* $\mathrm{M\overline{ed}\,P}$*,* $\mathrm{Med\,P}$ *und* $\mathrm{Mid\,P}$ *die gleichen harten Probleme bezüglich* $\leq_m^{\mathrm{FP}}$*, so folgt:* $\Sigma_2^p \subseteq \mathrm{PP}$ *und* $\mathrm{CH} = \mathrm{P}^{\mathrm{PP}}$*.*

Insbesondere (vgl. die Bemerkungen nach Korollar 3.17) gibt es also relativierte Welten, in denen die Mediaklassen unterschiedliche $\leq_m^{\mathrm{FP}}$-harte Probleme besitzen.

Wir wenden uns nun der Angabe natürlicher vollständiger Probleme für die verschiedenen Medianklassen unter funktionaler many-one-Reduzierbarkeit zu. Es wird sich dabei herausstellen, daß es sich im wesentlichen um Variationen der Probleme handelt, die Toda bereits in [Tod90] untersuchte und von denen wir zeigten, daß sie hart sind für alle betrachteten Medianklassen unter metrischen Reduktionen. Wir zeigen jetzt, daß leichte Modifikationen von ihnen vollständig sind für *verschiedene* Medianklassen unter $\leq_m^{\mathrm{FP}}$. Verschiedene Probleme charakterisieren also verschiedenen Medianklassen. Wir sehen dies als zusätzliche Rechtfertigung für die Untersuchung der von uns definierten Klassen an.

Wir möchten zwei Bemerkungen zur Darstellung vorausschicken:

Zum ersten handelt es sich bei den Methoden, die wir in unseren Beweisen verwenden, um „Standardtricks", die immer wieder in Vollständigkeitsbeweisen eine Rolle spielen. Die meisten von ihnen findet man in Lehrbüchern wie [GaJo79, PaSt82]. Wir werden im folgenden *nicht* die wohlbekannten Konstruktionen wiedergeben und ihre Korrektheit begründen (der Leser kann dies in den angegebenen Werken nachlesen), sondern nur die Punkte herausstellen, an denen sich unsere Argumentation von der in der Literatur unterscheidet.

Zum zweiten wird es (wie fast immer bei Vollständigkeitsbeweisen) meist so sein, daß die Mitgliedschaft des untersuchten Problems in der betreffenden Klasse oft einfach ist und die anzugebende Reduktion die eigentliche Schwierigkeit darstellt. Ist der erste Punkt zu trivial, verzichten wir daher stillschweigend auf eine Begründung.

Vollständige Probleme für $\mathrm{M\overline{ed}\,P}$

Mit Hilfe der Funktion $\textsc{Univ}_{\mathrm{M\overline{ed}P}}$ läßt sich recht einfach ein schaltkreistheoretisches vollständiges Problem für $\mathrm{M\overline{ed}\,P}$ angeben. Bei Eingabe $(x, \langle M\rangle, j, 0^k)$ suchen wir das mittlere Element unter allen $|y| \in [j]$, so daß (x, y) von der Maschine M in höchstens k Schritten akzeptiert wird. Wir können nun direkt einen Schaltkreis C_x angeben, der soviele Eingänge hat, wie Bits benötigt werden, um alle Werte aus $[j]$ darzustellen, und der eine Eingabe y genau dann akzeptiert, wenn sie aus $[j]$ ist und wenn M in höchstens k Schritten das Paar (x, y) akzeptiert. wird. Diese Konstruktion ist in Polynomialzeit durchführbar [Lad75, Sch86, BaDiGa88].

Wir erhalten also folgendes Resultat:

Problem:	LexMidCVal
Gegeben:	ein boolescher Schaltkreis C mit n Eingängen
Gesucht:	der lexikographisch mittlere String unter allen Strings der Länge n, der von C akzeptiert wird

3.32 Satz. LexMidCVal *ist* $\leq_m^{\mathrm{FP}}$*-vollständig für* $\mathrm{M\overline{ed}\,P}$.

Beweis. Wir zeigten soeben, daß $\mathrm{Univ}_{\mathrm{M\overline{ed}\,P}} \leq_m^{\mathrm{FP}}$ LexMidCVal. □

Es bietet sich nun an, ein vergleichbares über aussagenlogische Formeln definiertes Problem („mittlere erfüllende Belegung“) zu untersuchen. Die Erfahrung zeigt, daß im Kontext der Polynomialzeit-Komplexität die meisten Probleme, die über Schaltkreise definiert sind, leicht durch Probleme, die über aussagenlogische Formeln definiert sind, ersetzt werden können. Zu entscheiden, ob ein gegebener Schaltkreis eine akzeptierte Eingabe besitzt, ist beispielsweise von gleicher Komplexität, wie zu entscheiden, ob eine aussagenlogische Formel eine erfüllende Belegung besitzt.

In unserem Falle ergibt sich jedoch folgendes Problem:

Im Satz von Cook [Coo71] wird die Arbeitsweise von nichtdeterministischen Turingmaschinen durch aussagenlogische Formeln beschrieben. Eine erfüllende Belegung der Formel entspricht dabei genau einem akzeptierenden Pfad der Maschine. In der Belegung gibt es gewisse Variablen, die direkt den nichtdeterministischen Wahlmöglichkeiten der Maschine entsprechen, und andere Variablen, die lokale Eigenschaften der Maschine beschreiben. Es gilt stets, daß in jeder erfüllenden Belegung die Belegung der Variablen dieser zweiten Sorte deterministisch in Polynomialzeit berechnet werden kann, wenn erst einmal die Belegung der Variablen der ersten Sorte feststeht (also wenn die nichtdeterministischen Wahlmöglichkeiten getroffen sind).

Wollen wir in dem Problem LexMidCVal den Schaltkreis durch eine Formel ersetzen, stoßen wir erneut auf dieses Phänomen: Die Formel, die dem Schaltkreis entspricht, ist einfach eine Konjunktion kleiner Formeln, die lokale Eigenschaften des Schaltkreises (Gatter für Gatter) beschreiben. Jedem Gatter entspricht eine aussagenlogische Variable, die in einer erfüllenden Belegung dann genau den Wert des Gatters bei der entsprechenden akzeptierten Eingabe annimmt.

Es gibt also gewisse Variablen, die den Eingängen des Schaltkreises entsprechen, und andere Variablen, die inneren Gattern entsprechen. Liegt die Belegung der Variablen der erste Sorte fest, so kann die Belegung der Variablen für innere Gatter leicht in Polynomialzeit Schritt für Schritt – analog der Schaltkreisauswertung – berechnet werden. Wir verzichten darauf, den Vervollständigkeitsalgorithmus genauer anzugeben. Wir bemerken lediglich, daß er natürlich stark darstellungsabhängig ist (d. h. abhängig von der Formulierung des Schaltkreises in aussagenlogischen Ausdrücken). Für allgemeine aussagenlogische Formeln (die nicht aus Schaltkreisen entstehen), kann ein derartiger Algorithmus nur dann existieren, wenn P = NP. Wir sind nun interessiert an der mittleren Eingabe, die vom Schaltkreis akzeptiert wird. Dieser mittleren Eingabe entspricht nun nicht die gesamte mittlere erfüllende Belegung, sondern nur ein Teil der Belegung, in gewissem Sinne der *entscheidende Teil* der Belegung, nämlich die Belegung eingeschränkt auf die Variablen, die Schaltkreiseingängen entsprechen.

Dies führt uns zu folgender Begriffsbildung:

3.33 Definition. Es sei F eine aussagenlogische Formel. V sei die Menge der in F vorkommenden Variablen. Eine Teilmenge $V_0 \subseteq V$ heißt Menge *externer* Variablen, falls folgendes gilt: Der oben skizzierte Vervollständigungsalgorithmus ist in der Lage, für jede erfüllende Belegung von F die Belegung der Variablen aus $V_1 =_{\text{def}} V \setminus V_0$ (die sog. *internen* Variablen bezogen auf V_0) aus der Belegung der Variablen aus V_0 zu berechnen. Eine Belegung von F bezogen auf V_0 ist eine Abbildung $b: V_0 \to \{\text{wahr}, \text{falsch}\}$. Der Wert von F unter b ergibt sich, indem wir zunächst erweitern zu einer Abbildung $b': V \to \{\text{wahr}, \text{falsch}\}$ und dann F unter b' wie gewohnt auswerten.

Im Satz von Cook ist also die Menge der Variablen, die den Nichtdeterminismus beschreiben, extern; und in der Simulation eines Schaltkreises ist die Menge der Variablen, die die Werte der Eingabegatter beschreiben, extern, und die Menge der Variablen, die internen Schaltkreisgattern entsprechen, intern. Die mittlere akzeptierte Eingabe eines Schaltkreises entspricht also genau der der mittleren erfüllenden Belegung des Schaltkreises bezogen auf die Variablen, die den Eingängen des Schaltkreises entsprechen. Die Belegungen sind dabei so zu ordnen, daß die Ordnung der externen Variablen untereinander die Ordnung der Eingabegatter des Schaltkreises wiederspieget. Damit erhalten wir folgendes Resultat:

Problem:	LexMidSat
Gegeben:	eine aussagenlogische Formel F, eine ausgezeichnete Menge V von Variablen von F

Gesucht:	die lexikographisch mittlere erfüllende Belegung von F bezogen auf V, falls V extern ist; irgendeine Belegung sonst.

3.34 Satz. LexMidSat *ist* $\leq_m^{\mathrm{FP}}$*-vollständig für* $\mathrm{M\overline{ed}\,P}$.

Beweis. Die obige Diskussion zeigt, daß LexMidCVal $\leq_m^{\mathrm{FP}}$ LexMidSat. □

Mit Standardmethoden kann man nun von einem verwandten Problem, genannt LexMid3Sat, bei dem nur Formeln in konjunktiver Normalform mit 3 Literalen pro Klausel berücksichtigt werden, zeigen, daß es $\leq_m^{\mathrm{FP}}$-vollständig für $\mathrm{M\overline{ed}\,P}$ ist.

Die Unterscheidung zwischen externen und internen Variablen findet sich auch in ähnlicher Form bei anderen Problemen wieder. Wir unterscheiden bei einem gegebenen Graphen G zwischen externen und internen Kanten, wenn ein möglicher Hamiltonscher Kreis durch G schon durch Mitgliedschaft der externen Kanten vollständig festgelegt wird. (Wir bemerken erneut, daß auch hier die Art der Darstellung von Formeln in Graphen eine wichtige Rolle spielt.) Wir beschreiben Hamiltonsche Kreise, indem wir zunächst die externen Kanten ordnen und dann durch eine Folge von Bits, eins für jede externe Kante, angeben, welche Kanten zum Kreis gehören. Die Ordnung auf den Hamiltonschen Kreisen wird nun definiert durch die lexikographische Ordnung auf den so gegebenen Beschreibungen.

Problem:	LexMidHamC
Gegeben:	ein ungerichteter Graph G, eine ausgezeichnete Menge E von Kanten
Gesucht:	der lexikographisch mittlere Hamiltonsche Kreis bezogen auf E, falls E extern ist, irgendeine Kantenfolge sonst.

3.35 Satz. LexMidHamC *ist* $\leq_m^{\mathrm{FP}}$*-vollständig für* $\mathrm{M\overline{ed}\,P}$.

Beweis. Man zeigt LexMidSat $\leq_m^{\mathrm{FP}}$ LexMidHamC. Der Beweis entspricht genau dem NP-Vollständigkeitsbeweis des assoziierten Entscheidungsproblems aus [PaSt82, Seiten 366ff], jedoch ersetzen wir den Klauselgraph aus [PaSt82, Abbildung 15-9] durch den Klauselgraph aus [Tod90, Abbildung 4.2], da letzterer nur einen möglichen Hamiltonschen Pfad zuläßt. Genaue Erläuterungen findet man an den angegebenen Orten. Die Anwesenheit/Abwesenheit einzelner Kanten entspricht nun genau den Belegungen gewisser Variablen. Die Kanten, die externen Variablen entsprechen, bilden damit die entscheidende Menge der externen Kanten des Graphen. □

Vollständige Probleme für Med P

Wenden wir uns nun der zweiten Mediianklasse zu. Es bietet sich natürlich erneut an, mit einem aussagenlogischen Problem zu beginnen.

Problem:	MedWeightSat
Gegeben:	eine aussagenlogische Formel F, in der die Variablen gewichtet sind
Gesucht:	die mittlere Zahl in der Folge aller Summen der Gewichte der wahren Variablen in erfüllenden Belegungen von F

3.36 Satz. MedWeightSat *ist* $\leq_m^{\mathrm{FP}}$*-vollständig für* Med P.

Beweis. (Vgl. [Kre88, Satz 2.1].)
Wir zeigen $\mathrm{Univ}_{\mathrm{Med\,P}} \leq_m^{\mathrm{FP}}$ MedWeightSat. Gegeben eine Turingmaschine M und ein Eingabewort x, definiere eine Formel F derart, daß eine 1:1-Beziehung zwischen akzeptierenden Pfaden von M bei Eingabe x und erfüllenden Belegungen von F besteht. In diesen Belegungen gibt es Variablen, die direkt den Bits der Ausgabe von M entsprechen. Wir wichten alle anderen Variablen mit 0 und die Variablen, die Ausgaben entsprechen, so, daß die Summe insgesamt genau den Wert der Ausgabe widerspiegelt. Dann entspricht das Gewicht einer erfüllenden Belegung genau der Ausgabe auf dem entsprechenden Pfad der Maschine. □

Ideen von Krentel folgend können wir dieses Problem leicht auf zwei weitere reduzieren. Unsere Konstruktionen entsprechen genau denen vom Beweis von [Kre88, Satz 2.1].

Problem:	MedKnapsack
Gegeben:	ganze Zahlen $x_1, \ldots, x_n, M, N$
Gesucht:	die mittlere Summe $\sum_{i \in S} x_i - M$ in der Folge der Summen über alle $S \subseteq \{1, \ldots, n\}$, die einen Wert zwischen 0 und $N - M$ ergeben

3.37 Satz. MedKnapsack *ist* $\leq_m^{\mathrm{FP}}$*-vollständig für* Med P.

Beweis. Wir zeigen MedWeightSat $\leq_m^{\mathrm{FP}}$ MedKnapsack unter Verwendung von Standard-Knapsack-Kodierungstricks wie schon erwähnt wie in [Kre88, Satz 2.1]. Krentels Konstruktion hat die Eigenschaft, daß für geeignete M und N eine Lösung des Rucksack-Problems, die eine Summe zwischen M und N ergibt, direkt einer erfüllenden Belegung entspricht. Krentel benutzte nun metrische Reduktionen, um von der Summe den Wert M zu subtrahieren. Diese Möglichkeit haben wir hier nicht. Jedoch läßt sich der gleiche Effekt durch eine negative Vorgewichtung jeder möglichen Lösung erreichen, die wir direkt in die Definition des Problems mit aufgenommen haben. □

Problem:	MEDTSPTOUR
Gegeben:	ein ungerichteter, gewichteter Graph G
Gesucht:	die Länge der mittleren Handlungsreisenden-Tour in der Folge aller möglichen Touren gemäß G

3.38 Satz. MEDTSPTOUR *ist* $\leq_m^{\mathrm{FP}}$*-vollständig für* Med P.

Beweis. Wir zeigen MEDWEIGHTSAT $\leq_m^{\mathrm{FP}}$ MEDTSPTOUR. Die Konstruktion ähnelt einer aus [Kre88, Satz 2.1]. Wir benötigen hier jedoch nicht die C_k−false-Kanten. Wir wichten stattdessen die $C_k - y$-Kanten entsprechend dem Gewicht der Variablen y. □

Vollständige Probleme für Mid P

Erneut beginnen wir mit einem aussagenlogischen Problem. Dazu führen wir eine eingeschränkte Variante von QBF [BaDiGa88] ein (vgl. auch Schönings QBF_1-Formeln [Sch86]):

3.39 Definition. Eine Σ_1-Formel ist quantifizierte boolesche Formel, in der keine Universalquantoren vorkommen. Eine Belegung einer Σ_1-Formel ist eine Abbildung, die den freien Variablen in F einen Wahrheitswert zuordnet. Eine Belegung ist erfüllend, falls sie zu einer Abbildung fortgesetzt werden kann, die allen Variablen einen Wahrheitswert zuordnet und die die zugrundeliegende aussagenlogische Formel erfüllt.

Problem:	LEXMIDΣ_1SAT
Gegeben:	eine Σ_1-Formel F
Gesucht:	the lexikographisch mittlere erfüllende Belegung von F

3.40 Satz. LEXMIDΣ_1SAT *ist* $\leq_m^{\mathrm{FP}}$*-vollständig für* Mid P.

Beweis. $\textsc{LexMid}\Sigma_1\textsc{Sat} \in \mathrm{Mid\,P}$: Wir nutzen den Nichtdeterminismus der Turingmaschine, um sowohl für die freien als auch für die gebundenen Variablen einen Wahrheitswert zu raten. Kommen wir so zu einer erfüllenden Belegung der zugrundeliegenden aussagenlogischen Formel, so geben wir diese, eingeschränkt auf die freien Variablen, aus.

$\textsc{Univ}_{\mathrm{Mid\,P}} \leq_m^{\mathrm{FP}} \textsc{LexMid}\Sigma_1\textsc{Sat}$: Gegeben eine Maschine M und eine Eingabe x, konstruiere eine Formel F mit freien Variablen $y_1, \ldots, y_m$ mit folgender Bedeutung: $F(y_1, \ldots, y_m)$ ist genau dann wahr, wenn es einen akzeptierenden Pfad von M bei Eingabe x gibt, auf dem $y_1 \cdots y_m$ ausgegeben wird. □

Die drei Probleme, von denen wir zeigten, daß sie vollständig für Med P sind, sind definiert durch Finden des mittleren Elements einer Folge von Zahlen mit bestimmten Eigenschaften. Ersetzen wir in dieser Definiton „Folge“ durch „Menge“, kommen wir zu Problemen, von denen wir völlig analog zu den Beweisen von oben zeigen können, daß sie vollständig sind für Mid P.

Problem:	MidWeightSat
Gegeben:	eine aussagenlogische Formel F, in der die Variablen gewichtet sind
Gesucht:	die mittlere Zahl in der Menge aller Summen der Gewichte der wahren Variablen in erfüllenden Belegungen von F

Problem:	MidKnapsack
Gegeben:	ganze Zahlen $x_1, \ldots, x_n, M, N$
Gesucht:	die mittlere Summe $\sum_{i \in S} x_i - M$ in der Menge der Summen über alle $S \subseteq \{1, \ldots, n\}$, die einen Wert zwischen 0 und $N - M$ ergeben

Problem:	MidTSPTour
Gegeben:	ein ungerichteter, gewichteter Graph G
Gesucht:	die Länge der mittleren Handlungsreisenden-Tour in der Menge aller möglichen Touren gemäß G

3.41 Korollar. MidWeightSat, MidKnapsack *und* MidTSPTour *sind* $\leq_m^{\mathrm{FP}}$*-vollständig für* Mid P.

3.4. Vollständigkeitsresultate für Mengenklassen

Der Begriff der funktionalen many-one-Reduzierbarkeit erlaubt es uns, auf systematische Art und Weise aus den vollständigen Funktionen der letzten Klassen vollständige Mengen für die Klassen PP, $\mathrm{PP}^{\mathrm{NP}}$ sowie P^{PP} zu gewinnen.

Dazu beweisen wir zwei generische Sätze.

3.42 Satz.

1. *Ist* f $\leq_m^{\mathrm{FP}}$*-vollständig für* $\overline{\mathrm{Med}}\,\mathrm{P}$ *oder* $\mathrm{Med}\,\mathrm{P}$*, so ist* $\{\,(x,k) \mid f(x) \geq k\,\}$ $\leq_m^{\mathrm{P}}$*-vollständig für* PP*.*

2. *Ist* f $\leq_m^{\mathrm{FP}}$*-vollständig für* $\mathrm{Mid}\,\mathrm{P}$*, so ist* $\{\,(x,k) \mid f(x) \geq k\,\}$ $\leq_m^{\mathrm{P}}$*-vollständig für* $\mathrm{PP}^{\mathrm{NP}}$*.*

Beweis.

1. Aus Satz 3.16, Aussage 2, folgt direkt, daß $\{\,(x,k) \mid f(x) \geq k\,\} \in \mathrm{PP}$ für alle $f \in \overline{\mathrm{Med}}\,\mathrm{P} \cup \mathrm{Med}\,\mathrm{P}$.

   Sei nun f vollständig für $\overline{\mathrm{Med}}\,\mathrm{P}$ unter $\leq_m^{\mathrm{FP}}$. Sei $A \in \mathrm{PP}$. Dann gibt es also eine Funktion $h \in \mathrm{Med}\,\mathrm{P}$ und eine Funktion $g \in \mathrm{FP}$ so daß für alle x gilt: $x \in A$ genau dann, wenn $h(x) \geq g(x)$. Da f vollständig ist, gibt es eine Funktion $g' \in \mathrm{FP}$, so daß für alle x gilt: $h(x) = f(g'(x))$. Daraus folgt:
   $$\begin{aligned} x \in A &\iff f(g'(x)) \geq g(x) \\ &\iff (g'(x), g(x)) \in \{\,(x,k) \mid f(x) \geq k\,\} \end{aligned}$$
   Also reduziert die Funktion $g'' \in \mathrm{FP}$ mit $g''(x) =_{\mathrm{def}} (g'(x), g(x))$ die Menge A auf $\{\,(x,k) \mid f(x) \geq k\,\}$.

   Der Beweis für $\mathrm{Med}\,\mathrm{P}$ ist vollkommen analog.

2. Analog zum Beweis von 1. Jedoch benutzen wir nun Satz 3.16, Aussage 3.

$\square$

3.43 Satz. *Ist* f $\leq_m^{\mathrm{FP}}$*-vollständig für* $\overline{\mathrm{Med}}\,\mathrm{P}$, $\mathrm{Med}\,\mathrm{P}$ *oder* $\mathrm{Mid}\,\mathrm{P}$*, so ist* $\{\,x \mid f(x) \equiv 1 \pmod 2\,\}$ $\leq_m^{\mathrm{P}}$*-vollständig für* P^{PP}*.*

Beweis. Sei $f \in \overline{\mathrm{Med}}\,\mathrm{P} \cup \mathrm{Med}\,\mathrm{P} \cup \mathrm{Mid}\,\mathrm{P}$. Dann ist $\{\,x \mid f(x) \equiv 1 \pmod 2\,\} \in \mathrm{P}^{\mathrm{PP}}$. Man bestimme einfach das mittlere Element mittels binärer Suche und akzeptiere die Eingabe genau dann, wenn es ungerade ist.

Sei nun f vollständig für $\mathrm{M\overline{ed}\,P}$ (die Beweise in den anderen Fällen sind analog). Sei $A \in \mathrm{P}^{\mathrm{PP}}$. Dann ist $c_A \in \mathrm{FP}^{\mathrm{PP}}$. Aus dem Beweis von Satz 3.11 ergibt sich die Existenz einer $\mathrm{M\overline{ed}\,P}$-Funktion h ($h(x)$ ist das mittlere y mit $(x, y) \in B$) mit der Eigenschaft, daß wir dem Wert $h(x)$ den Wert $c_A(x)$ ablesen können. Genaueres Hinsehen ergibt, daß stets folgendes erreicht werden kann: $c_A(x) = 1 \iff h(x) \equiv 1 \pmod 2$.

Da f vollständig ist, gibt es eine Funktion $g' \in \mathrm{FP}$, so daß für alle x gilt: $h(x) = f(g'(x))$. Daraus folgt:

$$\begin{aligned} x \in A &\iff f(g'(x)) \equiv 1 \pmod 2 \\ &\iff g'(x) \in \{\, x \mid f(x) \equiv 1 \pmod 2 \,\} \end{aligned}$$

Also reduziert die Funktion g' die Menge A auf $\{\, x \mid f(x) \equiv 1 \pmod 2 \,\}$. $\square$

Alle in Abschnitt 3.3.2 betrachteten Probleme führen also zu vollständigen Mengen für PP oder $\mathrm{PP}^{\mathrm{NP}}$ sowie P^{PP}. Unter anderem erhalten wir so die (unseres Wissens nach) ersten natürlichen vollständigen Probleme für $\mathrm{PP}^{\mathrm{NP}}$, die nicht vollständig sind aufgrund der Eingaberepräsentation durch eine Input-Sprache (wie die in [Wag86a] angegebenen Probleme), sondern aufgrund ihrer eigenen inhärenten Komplexität.

4

Abstrakte Polynomialzeit-Komplexitätsklassen

Wir werden in den folgenden Kapiteln das Ziel verfolgen, systematisch eine Komplexitätstheorie von Funktionenklassen zu entwickeln. Es stellt sich nun die Frage, welche Mengen von Funktionen wir überhaupt untersuchen wollen, d. h. welche Eigenschaften Mengen von Funktionen haben sollen, damit sie „interessante Komplexitätsklassen“ ergeben, über die man fundierte strukturelle Aussagen machen kann.

Um unser Vorgehen zu motivieren, wenden wir uns zunächst der Mengenseite zu, da Komplexitätsuntersuchungen von Mengen ein vertrautes Gebiet darstellen. Zumindest im Rahmen der Polynomialzeit-Komplexität wird man sicherlich von einer Klasse von Mengen fordern, daß sie unter many-one-Reduktionen abgeschlossen ist. Ansonsten wird man kaum geneigt sein, solch ein Mengenensemble als Komplexitätsklasse zu betrachten. Es ist jedoch möglich, neben dieser Anforderung weitere „Axiome“ zu benennen, die, wie ein Blick in die Literatur zeigt, genau die Eigenschaften fordern, die in einer Reihe für uns relevanter Einzelresultate in der Vergangenheit ausgenutzt wurden.

4.1 Definition. Eine Klasse $\mathcal{K}$ von Mengen ist eine *abstrakte Polynomialzeit-Komplexitätsklasse (APK)*, falls gilt:

1. $\mathrm{P} \subseteq \mathcal{K}$.
2. $\mathcal{K}$ ist abgeschlossen unter Vereinigung und Durchschnitt.
3. $\mathcal{K}$ ist abgeschlossen under $\leq^{\mathrm{p}}_{dtt}$ und $\leq^{\mathrm{p}}_{ctt}$.

Man beachte, daß für Klassen $\mathcal{K}$, die unter markierter Vereinigung abgeschlossen sind, die Bedingung 2 aus der Bedingung 3 folgt. Umgekehrt ist eine APK offensichtlich unter markierter Vereinigung abgeschlossen. Es gilt also:

4.2 Beobachtung. *Eine Klasse $\mathcal{K}$ von Mengen ist genau dann eine APK, falls $\mathrm{P} \subseteq \mathcal{K}$ und falls $\mathcal{K}$ abgeschlossen ist unter markierter Vereinigung, $\leq^{\mathrm{p}}_{dtt}$ und $\leq^{\mathrm{p}}_{ctt}$.*

Genauso offensichtlich ist, daß der Punkt 3 äquivalent durch die Forderung nach Abschluß unter $\leq^{\mathrm{P}}_{bd\text{-}ptt}$ ersetzt werden kann.

Die folgenden Klassen sind APKs: P, NP, Σ^p_k, Π^p_k, Δ^p_k und Θ^p_k für alle $k \in \mathbb{N}$, $\oplus$P, PP, PH, CH, PSPACE. Natürlich sind nicht alle vertrauen Komplexitätsklassen APKs; z. B. erfüllen vermutlich die einzelnen Stufen der Booleschen Hierarchie über NP oder anderen Klassen und die Mod-Klassen [BeGiHe90, Her90] nicht die Bedingungen 2 und 3. Jedoch sind die APK-Bedingungen genau die Forderungen, die für eine Reihe von bekannten Resulten der Komplexitätstheorie verantwortlich sind.

4.3 Satz. *Ist $\mathcal{K}$ eine APK, so gilt:*

1. $\#\mathrm{P}^{\mathcal{K}} = \#(\mathcal{K} \wedge \text{co-}\mathcal{K})$.
2. $\mathrm{NP}^{\mathcal{K}} = \exists(\mathcal{K} \wedge \text{co-}\mathcal{K})$, $\text{co-NP}^{\mathcal{K}} = \forall(\mathcal{K} \wedge \text{co-}\mathcal{K})$ *und* $\mathrm{PP}^{\mathcal{K}} = \mathrm{C}(\mathcal{K} \wedge \text{co-}\mathcal{K})$.
3. $\mathrm{C}(\mathcal{K} \wedge \text{co-}\mathcal{K})$ *ist unter Durchschnitt abgeschlossen.*
4. $\mathrm{PH}(\mathcal{K} \wedge \text{co-}\mathcal{K}) \subseteq \mathrm{P}^{\#(\mathcal{K} \wedge \text{co-}\mathcal{K})}[1]$.

Beweis. Die Behauptungen wurden für verschiedene Spezialfälle bewiesen in [Li93, Tor91, BeReSp90, Tod91]. Die Eigenschaften der Klasse $\mathcal{K}$, die in diesen Beweisen benötigt werden, sind jedoch genau die APK-Bedingungen. □

Die obige Liste ist bei weitem nicht vollständig. Sie läßt sich erweitern um Resultate betreffend den BP-Operator [Sip83, Lau83], die Zählklassen #P [Her90, BeGiHe90, KSTT92] und Gap-P [FeFoKu91] und allgemeine Eigenschaften von Zählklassen (siehe dazu auch Kapitel 6; insbesondere Satz 6.3), Zensus-Technik und Fragen an dünne Mengen [Kad87], und viele mehr.

Sehr viele Resultate der strukturellen Komplexitätstheorie und bisher entwickelte Methoden und Beweistechniken hängen also nur von den APK-Eigenschaften der untersuchten Klassen ab. Es ist aber offensichtlich, daß man auf diese Art und Weise von einer Klasse $\mathcal{K}$ nie zeigen können wird, daß $\mathcal{K} \neq \exists\mathcal{K}$, denn es gibt APKs (z. B. PSPACE oder PH), für die $\mathcal{K} = \exists\mathcal{K}$. $\mathcal{K} \neq \exists\mathcal{K}$ kann also nicht nur aufgrund der APK-Eigenschaften von $\mathcal{K}$ bewiesen werden. Insbesondere wird man also, um das $\mathrm{P} \stackrel{?}{=} \mathrm{NP}$-Problem lösen zu können, Beweismethoden finden müssen, die über die meisten bisher bekannten (und über alle in den soeben zitierten Arbeiten verwendeten) hinausgehen.

In der Theorie der formalen Sprachen hat sich in den sechziger Jahren eine ähnliche Begriffsbildung herauskristallisiert: Eine Klasse von Sprachen über dem Alphabet Σ heißt *abstrakte Sprachfamilie (AFL)* genau dann, wenn sie Σ^*

enthält und abgeschlossen ist unter ε-freien Homomorphismen, inversen Homomorphismen, Schnitt mit regulären Mengen, Vereinigung, Konkatenation und Iteration. Es stellte sich dort ebenfalls heraus, daß eine Reihe von Ergebnissen, die bis dahin als Einzelresultate vorlagen, bereits für AFLs gültig sind. Interessanterweise gibt es eine enge Verbindung zwischen den Begriffen APK und AFL:

4.4 Satz. *Sei $\mathcal{K}$ eine Klasse von Mengen. Dann sind die folgenden Aussagen äquivalent:*

1. *$\mathcal{K}$ ist eine abstrakte Polynomialzeit-Komplexitätsklasse, die unter Existenzquantifizierung ($\exists$) abgeschlossen ist.*
2. *$\mathcal{K}$ ist eine abstrakte Sprachfamilie, die unter many-one-Reduktionen abgeschlossen ist.*

Beweis.
(1) $\Rightarrow$ (2): Sei $\mathcal{K}$ eine APK mit $\exists\mathcal{K} = \mathcal{K}$. Wir zeigen, daß $\mathcal{K}$ eine AFL ist.

- $\Sigma^* \in \mathrm{P}$, also auch $\Sigma^* \in \mathcal{K}$.
- Sei $A = h(B)$ für eine Menge $B \in \mathcal{K}$ und einen ε-freien Homomorphismus h. Dann gilt:
$$\begin{aligned} x \in A &\iff \exists y(y \in B \wedge x = h(y)) \\ &\iff \exists y(|y| \leq |x| \wedge (x,y) \in \{\,(x,y) \mid y \in B\,\} \\ &\qquad\qquad\qquad\qquad \cap \{\,(x,y) \mid x = h(y)\,\}) \end{aligned}$$
Also ist $A \in \exists\mathcal{K} = \mathcal{K}$.
- Sei $A = h^{-1}(B)$ für einen Homomorphismus h und eine Menge $B \in \mathcal{K}$. Dann gilt offensichtlich: $A \leq_m^{\mathrm{p}} B$, also $A \in \mathcal{K}$.
- Reguläre Mengen sind in $\mathrm{P} \subseteq \mathcal{K}$, also ist $\mathcal{K}$ abgeschlossen unter Schnitt mit regulären Mengen.
- $\mathcal{K}$ ist nach Voraussetzung abgeschlossen unter Vereinigung.
- Sei $A = B \cdot C$ für $B, C \in \mathcal{K}$. $\mathcal{K}$ ist abgeschlossen unter markierter Vereinigung, also ist die Menge D in $\mathcal{K}$, die folgendermaßen definiert ist: $D =_{\mathrm{def}} 0B \cup 1C$. Nun gilt:
$$\begin{aligned} x \in A &\iff \exists y \exists z(x = yz \wedge x \in B \wedge y \in C) \\ &\iff \exists y \exists z(|y| \leq |x| \wedge |z| \leq |x| \wedge \\ &\qquad (x,y,z) \in \{\,(x,y,z) \mid x = yz\,\} \\ &\qquad\qquad \cap \{\,(x,y,z) \mid 0y \in D\,\} \\ &\qquad\qquad \cap \{\,(x,y,z) \mid 1z \in D\,\}) \end{aligned}$$
Also folgt $A \in \exists\mathcal{K} = \mathcal{K}$.

- Sei $A = B^*$ für $B \in \mathcal{K}$. Es gilt:

$$\begin{array}{rcl} x \in A & \iff & \exists z_1\#z_2\#\cdots\#z_m(x = z_1z_2\cdots z_m \wedge z_1,\ldots,z_m \in B) \\ & \iff & \exists y(|y| \leq 2|x| \wedge (x,y) \in \\ & & \quad \{(x, z_1\#z_2\#\cdots\#z_m) \mid x = z_1z_2\cdots z_m\} \cap \\ & & \quad \{(x, z_1\#z_2\#\cdots\#z_m) \mid z_1 \in B \wedge \ldots \wedge z_m \in B\} \end{array}$$

  Also folgt $A \in \exists\mathcal{K} = \mathcal{K}$.

(2) $\Rightarrow$ (1): Es sei $\mathcal{K}$ eine AFL mit $\mathcal{R}^{\mathrm{p}}_m(\mathcal{K}) = \mathcal{K}$. Wir zeigen zunächst, daß $\mathcal{K}$ eine APK ist.

- $\mathrm{P} = \mathcal{R}^{\mathrm{p}}_m(\{0\})$, $\{0\}$ ist aber regulär, also in $\mathcal{K}$. Damit folgt $\mathrm{P} \subseteq \mathcal{K}$.

- Sei $A = B \cap C$ für $B, C \in \mathcal{K}$. Dann gilt: $x \in A \iff x\#x \in B \cdot \{\#\} \cdot C$, also $A \leq^{\mathrm{p}}_m B \cdot \{\#\} \cdot C$. Da aufgrund der AFL-Bedingungen $B \cdot \{\#\} \cdot C \in \mathcal{K}$, folgt: $A \in \mathcal{K}$.

- $\mathcal{K}$ ist nach Voraussetzung abgeschlossen unter Vereinigung.

- Sei $A \leq^{\mathrm{p}}_{ctt} B$ für ein $B \in \mathcal{K}$. Dann gibt es eine Funktion $g \in \mathrm{FP}$, für die gilt:

$$\begin{array}{rcl} x \in A & \iff & z_1,\ldots,z_m \in B \qquad \text{wobei } g(x) = (z_1,\ldots,z_m) \\ & \iff & \#z_1\#\cdots\#z_m \in (\{\#\}\cdot B)^* \end{array}$$

  Diese letzte Menge ist aber aufgrund des Abschlusses von $\mathcal{K}$ unter den AFL-Operationen auch in $\mathcal{K}$.

- Sei $A \leq^{\mathrm{p}}_{dtt} B$ für ein $B \in \mathcal{K}$. Dann gibt es eine Funktion $g \in \mathrm{FP}$, für die gilt:

$$\begin{array}{rcl} x \in A & \iff & \{z_1,\ldots,z_m\} \cap B \neq \emptyset \qquad \text{wobei } g(x) = (z_1,\ldots,z_m) \\ & \iff & \#z_1\#\cdots\#z_m \in (\{\#\}\cdot\Sigma^*)^* \cdot \{\#\} \cdot B \cdot (\{\#\}\cdot\Sigma^*)^* \end{array}$$

  Diese letzte Menge ist aber aufgrund des Abschlusses von $\mathcal{K}$ unter den AFL-Operationen auch in $\mathcal{K}$.

Bleibt noch zu zeigen, daß $\exists\mathcal{K} = \mathcal{K}$.

Sei dazu A definiert durch $x \in A \iff \exists y(|y| = p(|x|) \wedge (x,y) \in B)$ für ein $B \in \mathcal{K}$ und ein Polynom p. Definiere $A_1 =_{\mathrm{def}} \{x\#^{p(|x|)-|x|} \mid x \in A\}$. Dann gilt: $A \leq^{\mathrm{p}}_m A_1$, $x \in A \iff g_0(x) =_{\mathrm{def}} x\#^{p(|x|)-|x|} \in A_1$. Sei $g =_{\mathrm{def}} g_0^{-1}$. Offensichtlich ist $g \in \mathrm{FP}$.

Dann gilt:

$$\begin{aligned} z \in A_1 &\iff z = g(z)\#^{p(|g(z)|)-|g(z)|} \wedge g(z) \in A \\ &\iff z = g(z)\#^{p(|g(z)|)-|g(z)|} \wedge \exists y(|y| = |z| \wedge (g(z), y) \in B) \\ &\iff \exists y(|y| = |z| \wedge z = g(z)\#^{p(|g(z)|)-|g(z)|} \wedge (g(z), y) \in B) \end{aligned}$$

Definiere folgende Menge:

$$B_1 =_{\mathrm{def}} \{ (y, z) \mid |y| = |z| \wedge z = g(z)\#^{p(|g(z)|)-|g(z)|} \wedge (g(z), y) \in B \}.$$

Offensichtlich ist $B_1 \leq_m^{\mathrm{p}} B$; also ist $B_1 \in \mathcal{K}$. Nun folgt:

$$\begin{aligned} z \in A_1 &\iff \exists y(|y| = |z| \wedge (y, z) \in B_1) \\ &\iff \exists u(u \in B_2 \wedge z = h(u)), \end{aligned}$$

wobei

$$B_2 =_{\mathrm{def}} \{ (a_1, b_1), (a_2, b_2), \ldots, (a_m, b_m) \mid (a_1 a_2 \cdots a_m, b_1 b_2 \cdots b_m) \in B_1 \}.$$

Offensichtlich ist $B_2 \leq_m^{\mathrm{p}} B_1$, also ist $B_2 \in \mathcal{K}$. Der Homomorphismus h in der Definition von A_1 ist definiert als $h((a, b)) =_{\mathrm{def}} a$.

Nun ergibt sich $A_1 = h(B_2)$; daraus folgt $A \in \mathcal{K}$. $\square$

5

Optimierungsfunktionen

Wir wenden uns in diesem Kapitel Funktionenklassen zu, die über einen Optimierungsprozeß definiert sind. Zunächst untersuchen wir einige konkrete Operatoren, die Optimierungsklassen bilden, und danach abstrahieren wir von speziellen Eigenschaften dieser Operatoren und entwickeln eine allgemeine Theorie von Optimierungsklassen.

5.1. Funktionentheoretische Operatoren

Wir führen in diesem Abschnitt Operatoren ein, die die Prinzipien der Definitionen der Klassen Opt P [Kre88] und Med P (siehe Kapitel 3) verallgemeinern, und wir geben einige einfache Beziehungen zwischen ihnen an. Unsere Wahl fiel auf Med P anstelle von Mid P, weil die erste Klasse eine „reinere" Medianklasse ist. In Mid P wird die Medianbildung mit einem zusätzlichen Existenzquantor „vermischt" (siehe Abbildung 3.2).

5.1 Definition. Es sei $\mathcal{F}$ eine Klasse von Funktionen. Dann definieren wir:

$$\begin{array}{lcl} h \in \mathrm{Max}\,\mathcal{F} & \iff & \text{es gibt } f \in \mathcal{F}, g \in \mathrm{FP} \text{ so daß} \\ & & h(x) = \max_{0 \leq y \leq g(x)} f(x,y) \\ h \in \mathrm{Min}\,\mathcal{F} & \iff & \text{es gibt } f \in \mathcal{F}, g \in \mathrm{FP} \text{ so daß} \\ & & h(x) = \min_{0 \leq y \leq g(x)} f(x,y) \\ h \in \text{r-Med}\,\mathcal{F} & \iff & \text{es gibt } f \in \mathcal{F}, g \in \mathrm{FP} \text{ so daß} \\ & & h(x) = \text{r-med}_{0 \leq y \leq g(x)} f(x,y) \\ h \in \text{l-Med}\,\mathcal{F} & \iff & \text{es gibt } f \in \mathcal{F}, g \in \mathrm{FP} \text{ so daß} \\ & & h(x) = \text{l-med}_{0 \leq y \leq g(x)} f(x,y) \end{array}$$

Für eine Multimenge M ist dabei r-med M der „Rechts-Median" von M, d. h. falls $M = \{m_1, m_2, \ldots, m_k\}$, $m_1 \leq m_2 \leq \cdots \leq m_k$, so ist r-med $M =_{\mathrm{def}} m_{\lceil (k+1)/2 \rceil}$. Analog ist l-med M, der „Links-Median", obiger Menge definiert als l-med $M =_{\mathrm{def}} m_{\lceil k/2 \rceil}$. Die Klasse Med $\mathcal{F}$ bezeichnet nun die Vereinigung der Klassen r-Med $\mathcal{F}$ und l-Med $\mathcal{F}$.

Wir werden erneut oft abkürzend $y \leq g(x)$ anstelle von $0 \leq y \leq g(x)$ schreiben. Weiterhin verwenden wir die Schreibweise $\mathrm{med}_{y \leq g(x)} f(x, y)$, um anzudeuten, daß die betreffende Aussage sowohl im r-med- als auch im l-med-Falls gültig ist.

Die Funktionenklassen $\mathcal{F}$, die wir im Rest dieser Arbeit untersuchen, erfüllen stets $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$. Klarerweise ist für derartige Klassen die obige Definition äquivalent zu der Formulierung, in der wir den Bereich für y allgemeiner mit $g_1(x) \leq y \leq g_2(x)$ für $g_1, g_2 \in \mathrm{FP}$ festlegen.

Offensichtlich ist $\mathrm{Opt\,P} = \mathrm{Max\,FP} \cup \mathrm{Min\,FP}$ und $\mathrm{Med\,P} = \mathrm{Med\,FP}$.

Wir geben nun eine Reihe von Eigenschaften dieser Operatoren an, die im Rest dieser Arbeit immer wieder benötigt werden.

5.2 Lemma. *Ist $\mathcal{F}$ eine Funktionenklasse, die abgeschlossen ist unter Addition von FP_+-Funktionen, so gilt:*

1. *(a)* $\mathrm{Max}(\mathcal{F} - \mathrm{FP}) = \mathrm{Max}\,\mathcal{F} - \mathrm{FP}$.
   (b) $\mathrm{Min}(\mathcal{F} - \mathrm{FP}) = \mathrm{Min}\,\mathcal{F} - \mathrm{FP}$.
   (c) $\mathrm{Med}(\mathcal{F} - \mathrm{FP}) = \mathrm{Med}\,\mathcal{F} - \mathrm{FP}$.
2. *(a)* $\mathrm{Max}(-\mathcal{F}) = -\mathrm{Min}\,\mathcal{F}$ *und* $\mathrm{Max}(\mathrm{FP} - \mathcal{F}) = \mathrm{FP} - \mathrm{Min}\,\mathcal{F}$.
   (b) $\mathrm{Min}(-\mathcal{F}) = -\mathrm{Max}\,\mathcal{F}$ *und* $\mathrm{Min}(\mathrm{FP} - \mathcal{F}) = \mathrm{FP} - \mathrm{Max}\,\mathcal{F}$.
   (c) $\mathrm{Med}(-\mathcal{F}) = -\mathrm{Med}\,\mathcal{F}$ *und* $\mathrm{Med}(\mathrm{FP} - \mathcal{F}) = \mathrm{FP} - \mathrm{Med}\,\mathcal{F}$.

Beweis.

1. (a) Es sei $h \in \mathrm{Max}(\mathcal{F} - \mathrm{FP})$, $h(x) = \max_{y \leq g'(x)}(f(x, y) - g(x, y))$ für Funktionen $f \in \mathcal{F}$ und $g' \in \mathrm{FP}$, $g \in \mathrm{FP}$. Sei $g'' \in \mathrm{FP}$ monoton-wachsend im zweiten Argument mit der Eigenschaft $g''(x, y) \geq g(x, y)$. Setze $g_1(x) =_{\mathrm{def}} g''(x, g'(x))$. Sei $g_2 \in \mathrm{FP}_+$ mit der Eigenschaft $g(x, y) = g_1(x) - g_2(x, y)$. Dann gilt: $h(x) = \max_{y \leq g'(x)}(f(x, y) - g(x, y)) = \max_{y \leq g'(x)}(f(x, y) + g_2(x, y)) - g_1(x)$. Also ist $h \in \mathrm{Max}\,\mathcal{F} - \mathrm{FP}$.

   Ist umgekehrt $h(x) = (\max_{y \leq g'(x)} f(x, y)) - g(x)$ für Funktionen $f \in \mathcal{F}$ und $g' \in \mathrm{FP}$, $g \in \mathrm{FP}$, dann ist offensichtlich $h(x) = \max_{y \leq g'(x)}(f(x, y) - g(x))$, also $h \in \mathrm{Max}(\mathcal{F} - \mathrm{FP})$.

   (b), (c) Die Beweise verlaufen vollkommen analog zum Punkt (a).

2. (a) Wir beweisen die zweite Aussage. Der Beweis der ersten ist analog. Es sei $h \in \mathrm{Max}(\mathrm{FP} - \mathcal{F})$, $h(x) = \max_{y \leq g'(x)}(g(x, y) - f(x, y))$ für Funktionen $f \in \mathcal{F}$ und $g' \in \mathrm{FP}$, $g \in \mathrm{FP}$. Wie im Teil (a) oben wählen wir $g_1 \in \mathrm{FP}, g_2 \in \mathrm{FP}_+$, so daß $g(x, y) = g_1(x) - g_2(x, y)$.

Dann gilt: $h(x) = \max_{y \leq g'(x)}(g_1(x) - (f(x,y) + g_2(x,y))) = g_1(x) - \min_{y \leq g'(x)}(f(x,y) + g_2(x,y))$. Also ist $h \in \mathrm{FP} - \mathrm{Min}\,\mathcal{F}$.
Ist umgekehrt $h(x) = g(x) - \min_{y \leq g'(x)} f(x,y)$ für Funktionen $f \in \mathcal{F}$ und $g' \in \mathrm{FP}$, $g \in \mathrm{FP}$, dann ist offensichtlich $h(x) = \max_{y \leq g'(x)}(g(x) - f(x,y))$, also $h \in \mathrm{Max}(\mathrm{FP} - \mathcal{F})$.

(b) Analog zum Punkt (a).

(c) Analog zum Punkt (a). Man beachte, daß Rechts-Mediane in Links-Mediane umgewandelt werden und umgekehrt; da wir jedoch nur eine Aussage über die Vereinigungsklasse $\mathrm{Med}\,\mathcal{F}$ machen wollen, ist dies nicht weiter störend.

□

5.3 Lemma. *Ist $\mathcal{F}$ eine Funktionenklasse mit der Eigenschaft $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$, so gilt:*

1. $\mathrm{Max}\,\mathrm{Max}\,\mathcal{F} = \max(\mathrm{Max}\,\mathcal{F}, \mathrm{Max}\,\mathcal{F}) = \mathrm{Max}\,\mathcal{F}$.
2. $\mathrm{Min}\,\mathrm{Min}\,\mathcal{F} = \min(\mathrm{Min}\,\mathcal{F}, \mathrm{Min}\,\mathcal{F}) = \mathrm{Min}\,\mathcal{F}$.
3. $\min(\mathrm{Max}\,\mathcal{F}, \mathrm{Max}\,\mathcal{F}) \subseteq \mathrm{Max}\min(\mathcal{F}, \mathcal{F})$.
4. $\max(\mathrm{Min}\,\mathcal{F}, \mathrm{Min}\,\mathcal{F}) \subseteq \mathrm{Min}\max(\mathcal{F}, \mathcal{F})$.

Beweis. Wiederum verlaufen alle Beweise sehr ähnlich. Wir geben exemplarisch den Beweis von Punkt 3.

Es sei $h(x) =_{\mathrm{def}} \min\{f_1(x), f_2(x)\}$, $f_i(x) =_{\mathrm{def}} \max_{y < g_i(x)} f_i'(x,y)$ für Funktionen $f_i' \in \mathcal{F}$, $g_i \in \mathrm{FP}$ $(i = 1, 2)$. Dann ist

$$\begin{aligned} h(x) &= \max_{\substack{y_1 < g_1(x) \\ y_2 < g_2(x)}} \min\{f_1'(x,y_1), f_2'(x,y_2)\} \\ &= \max_{y < g_1(x) \cdot g_2(x)} \min\{f_1'(x, y \bmod g_1(x)), f_2'(x, y \div g_1(x))\} \end{aligned}$$

□

5.2. P-fundierte Klassen von Optimierungsfunktionen

Wir werden nun eine abstrakte Untersuchung von Optimierungsklassen beginnen, die die Eigenschaften der Operatoren Max, Min und Med verallgemeinern. Unser erstes Ziel ist die Erarbeitung einer Reihe von Bedingungen (ähnlich den

APK-Axiomen), die wir an Funktionenklassen stellen wollen. Dazu folgende Überlegungen:

Analog zum many-one-Abschluß von Mengenklassen sollten unsere Funktionenklassen sicherlich eine Bedingung erfüllen, die bereits in Lemma 5.3 gefordert wurde, nämlich $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$. Aus der Voraussetzung von Lemma 5.2 übernehmen wir die Forderung $\mathcal{F} + \mathrm{FP}_+ \subseteq \mathcal{F}$ und nehmen zusätzlich $\mathcal{F} \cdot \mathrm{FP}_+ \subseteq \mathcal{F}$ auf. Weiterhin hätten wir gerne analog zum ersten APK-Axiom, daß $\mathrm{FP} \subseteq \mathcal{F}$. Wenn $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$ gilt, genügt es also, nur zu fordern, daß die Identität id stets ein Element unserer Funktionenklassen ist. Weiterhin müssen wir sicherstellen, daß wir die Funktionen überhaupt in Polynomialzeit manipulieren können; wir fordern also, daß sie im Wert stets durch eine FP-Funktion beschränkt sind. Die Möglichkeit, Funktionen per Fallunterscheidung definieren zu können, ist ein funktionales Analogon zum Abschluß unter markierter Vereinigung; wir fordern also, daß uns Definition durch Fallunterscheidung nicht aus den betrachteten Klasen herausführt.

Neben den gerade genannten mehr technischen Bedingungen stellen wir zwei weitere, substantiellere Anforderungen:

Wir fordern, daß parallele Fragen an eine Funktion durch eine einzige Frage simuliert werden können. Denken wir zum Beispiel an eine Max FP-Funktion h. Dann gibt es eine nichtdeterministische Polynomialzeit-Turingmaschine M, so daß $h(x)$ gleich dem Maximum aller Ausgabewerte der Pfade der Rechnung von M bei Eingabe x ist. Wollen wir nun das Paar $\langle h(x), h(y)\rangle$ berechnen, so starten wir zunächst M bei Eingabe x; und in jeder haltenden Konfiguration starten wir sodann M bei Eingabe y. Hält M nun erneut, so geben wir als Resultat das Paar bestehend aus den beiden Einzelresultaten aus. Das maximale solche Paar ist dann genau der Wert $\langle h(x), h(y)\rangle$. Analoge Überlegungen lassen sich auch für Min-Klassen durchführen. Haben wir es mit Medianfunktionen zu tun, geraten wir jedoch in Schwierigkeiten. Eine Konstruktion analog zu der obigen führt nicht zum Ziel. Betrachten wir als Beispiel eine Med FP-Berechnung mit den Ausgabewerten $0, 1, 1$ und eine zweite Berechnung mit den Ausgabewerten $0, 1, 2$. Die Folge aller Paare ist dann $\langle 0,0\rangle$, $\langle 0,1\rangle$, $\langle 0,2\rangle$, $\langle 1,0\rangle$, $\langle 1,1\rangle, \langle 1,2\rangle$, $\langle 1,0\rangle$, $\langle 1,1\rangle, \langle 1,2\rangle$. Der Median dieser Folge ist $\langle 1,0\rangle$. Das Paar der beiden Einzelmediane ist jedoch $\langle 1,1\rangle$. Die schrittweise Bildung der Mediane ist also verschieden von der Medianbildung der Paare. (Im Gegensatz dazu ist die schrittweise Maximum- oder Minimumbildung identisch mit der Bildung von Maxima oder Minima über Paare.) Das Problem entsteht dann nicht, wenn die Werte in den einzelnen Folgen nur höchstens einmal auftreten, also eindeutig sind. Dann tritt eine Verschiebung wie im obigen Beispiel nicht auf. Im Falle Med FP können wir eindeutige Werte dadurch erreichen, daß wir neben dem eigentlichen Wert zusätzlich eine Kodierung des Berechnungspfades mit ausgeben. Was wir dann jedoch letzendlich als Ergebnis bekommen, ist nicht das Paar der Mediane, sondern das Paar der Mediane angereichert mit Werten, die uns nicht interessieren. Aber wir können diesem angereicherten Paar direkt die Werte, die uns interessieren, ablesen. Wir fordern, daß eine Tupelbildung, wie gerade beschrieben, in der Funktionenklasse möglich sein soll.

Alle bisher genannten Eigenschaften zeichnen jedoch noch nicht Optimierungsfunktionen aus. Sie treffen auch auf typische Klassen von Zählfunktionen, z. B. $\#$P und Gap-P zu. Optimierungsfunktionen in unserem Sinn sind, wie bereits in der Einleitung erläutert, gekennzeichnet durch einen Selektionsprozeß. Es wird ein Wert aus einer im allgemeinen exponentiell-großen Folge von Werten ausgewählt. Zählfunktionen entstehen im Gegensatz dazu durch eine Kombination der Werte dieser Folge, z. B. Summation. Gewisse Manipulationen der einzelnen Werte der Folge übertragen sich daher bei Optimierungsfunktionen auch direkt auf das ausgewählte Optimum. Bei Zählfunktionen ist das jedoch unter Umständen schwierig, da sich eben die einzelnen Manipulationen summieren können und nicht mehr trennen lassen. Es stellt sich heraus, daß diese Überlegung durch eine einfache Forderung zum Ausdruck gebracht werden kann: Wir fordern, daß Klassen von Optimierungsfunktionen abgeschlossen sind unter max- und min-Operationen mit FP-Funktionen. Betrachten wir zum Beispiel eine Med FP-Funktion h und eine FP-Funktion g. Um den Wert $\max\{h(x), g(x)\}$ zu bestimmen, starten wir die Maschine, die h berechnet, geben aber auf jedem Pfad anstelle des eigentlichen Ausgabewertes z nun den Wert $\max\{z, g(x)\}$ aus. Der Median über all diese neuen Werte ist nun tatsächlich das Maximum aus dem alten Median und dem Wert $g(x)$. Ähnliche Überlegungen gelten auch für Max FP sowie Min FP. Man beachte jedoch, daß die oben genannten Klassen von Zählfunktionen diese Abschlußeigenschaften nicht besitzen, es sei denn, die Counting-Hierarchie kollabiert auf XP.

Wir machen also folgende Definition:

5.4 Definition. Eine Funktionenklasse $\mathcal{F}$ ist eine *p-fundierte Klasse von Optimierungsfunktionen (PFO)*, falls die folgenden Bedingungen erfüllt sind:

1. Für $f \in \mathcal{F}$ existieren $g_1, g_2 \in \mathrm{FP}$, so daß für alle x gilt: $g_1(x) < f(x) < g_2(x)$.
   ($\mathcal{F}$ ist *polynomiell längenbeschränkt*)

2. $\mathrm{id} \in \mathcal{F}$.

3. $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$.
   (*Abschluß unter Eingabetransformationen*)

4. Ist $f \in \mathcal{F}$, $g \in \mathrm{FP}_+$, so ist $f + g, f \cdot g \in \mathcal{F}$.
   (*Abschluß unter Addition und Multiplikation mit* FP_+*-Funktionen*)

5. Ist $f_1, f_2 \in \mathcal{F}$, $A \in \mathrm{P}$, so ist die folgendermaßen definierte Funktion h ein Element von $\mathcal{F}$:

$$h(x) =_{\mathrm{def}} \begin{cases} f_1(x), & \text{falls } x \in A; \\ f_2(x), & \text{sonst.} \end{cases}$$

(*Abschluß unter Definition durch Fallunterscheidung*)

6. Für $f \in \mathcal{F}$, $g, g' \in \mathrm{FP}_+$, wobei $f(x,u) \in [g'(x)]$ für $u \in [g(x)]$, existieren $h \in \mathcal{F}$, $g'' \in \mathrm{FP}$, und r so daß $r(x,u) \in [g''(x)]$ für $u \in [g(x)]$, und für alle $m \in \mathbb{N}$, $u_1, \ldots, u_m \in [g(x)]$ gilt

$$\begin{aligned} &h(x, \langle u_1, \ldots, u_m\rangle_{g(x)}) = \\ &\quad \langle r(x,u_1), f(x,u_1), r(x,u_2), f(x,u_2), \ldots, f(x,u_m)\rangle_{g''(x), g'(x)}. \end{aligned}$$

(*Abschluß unter Tupelbildung*)

7. Ist $f \in \mathcal{F}$, $g \in \mathrm{FP}$, so ist $\min(f,g), \max(f,g) \in \mathcal{F}$.
(*Abschluß unter min-max-Operationen mit* FP-*Funktionen*)

Die Überlegungen, die wir vor Definition 5.4 machten, zeigen bereits, daß die Klassen Max FP, Min FP und Med FP PFOs sind. Wir werden als nächstes ein allgemeines Resultat angeben, daß aussagt, daß eine PFO $\mathcal{F}$ unter den drei Optimierungsoperatoren wieder in eine PFO überführt wird.

Zunächst benötigen wir jedoch zwei technische Resultate.

5.5 Lemma. *Sei $\mathcal{F}$ eine PFO. Dann gilt: Für alle $f \in \mathcal{F}$, $g, g' \in$* FP *wobei $g' > g$, existiert eine Funktion $f' \in \mathcal{F}$, so daß*

$$\max_{y \le g(x)} f(x,y) = \max_{y \le g'(x)} f'(x,y);$$

bzw. analog

$$\min_{y \le g(x)} f(x,y) = \min_{y \le g'(x)} f'(x,y),$$

$$\underset{y \le g(x)}{\text{r-med}}\, f(x,y) = \underset{y \le g'(x)}{\text{r-med}}\, f'(x,y),$$

$$\underset{y \le g(x)}{\text{l-med}}\, f(x,y) = \underset{y \le g'(x)}{\text{l-med}}\, f'(x,y).$$

Beweis. Seien $f \in \mathcal{F}$, $g, g' \in \mathrm{FP}$ wie in der Aussage des Lemmas gegeben. Sei $g_1 \in \mathrm{FP}$, so daß $g_1(x) \le f(x,y)$ für alle $y \le g(x)$. Definiere folgende Funktion f':

$$f'(x,y) = \begin{cases} f(x,y), & \text{falls } y \le g(x); \\ g_1(x), & \text{sonst.} \end{cases}$$

Dann gilt: $\max_{y \leq g(x)} f(x,y) = \max_{y \leq g'(x)} f'(x,y)$. Der Beweis für den Fall der Minimisierung verläuft analog.

Im r-Med-Fall definieren wir f' folgendermaßen: Sei g_1 wie oben und $g_2 \in \mathrm{FP}$ mit $f(x,y) \leq g_2(x)$ für alle $y \leq g(x)$.

$$f'(x,y) = \begin{cases} f(x,y), & \text{falls } y \leq g(x); \\ g_2(x), & \text{falls } y > g(x), y = 2i, i \in \mathbb{N}; \\ g_1(x), & \text{falls } y > g(x), y = 2i+1, i \in \mathbb{N} \end{cases}$$

Dann gilt: $\text{r-med}_{y \leq g(x)} f(x,y) = \text{r-med}_{y \leq g'(x)} f'(x,y)$. Der l-Med-Fall verläuft analog. $\square$

Dieses Lemma erlaubt es uns, bei der Kombination von zwei Funktionen, die über einen der obigen Operatoren definiert sind, ohne Beschränkung der Allgemeinheit davon auszugehen, daß der Bereich, über den die Operatoren rangieren, in beiden Fällen gleich ist.

Wir benötigen später ein technisches Lemma, das wir hier anschließen, weil sein Beweis ähnlich zum letzten Beweis verläuft.

5.6 Lemma. *Sei $\mathcal{F}$ eine PFO. Dann gilt:*

1. $\mathcal{F} \subseteq \mathrm{Min}\,\mathcal{F} \cap \mathrm{Max}\,\mathcal{F}$.
2. $\mathrm{Min}\,\mathcal{F} \cup \mathrm{Max}\,\mathcal{F} \subseteq \mathrm{Med}\,\mathcal{F}$.

Beweis. Aussage 1 ist trivial.

Sei $h \in \mathrm{Min}\,\mathcal{F}$, $h(x) = \min_{y<g(x)} f(x,y)$ für $f \in \mathcal{F}$, $g \in \mathrm{FP}$. Sei $g' \in \mathrm{FP}$ mit $g'(x) < f(x,y)$ für $y \leq g(x)$. Definiere folgende Funktion f':

$$f'(x,y) = \begin{cases} f(x,y), & \text{falls } y < g(x) \\ g'(x), & \text{sonst.} \end{cases}$$

Dann ist $h \in \mathcal{F}$ und $h(x) = \mathrm{med}_{y<2g(x)} f'(x,y)$. Der Max-Fall verläuft analog. $\square$

Wir kommen nun zum Hauptresultat dieses Abschnitts:

5.7 Satz.

1. FP *ist eine PFO.*
2. *Ist $\mathcal{F}$ eine PFO, so sind auch* $\mathrm{Max}\,\mathcal{F}$, $\mathrm{Min}\,\mathcal{F}$ *und* $\mathrm{Med}\,\mathcal{F}$ *PFOs.*

Beweis. Aussage 1 ist trivial.

Sei nun $\mathcal{F}$ eine PFO.

Ist $h \in \operatorname{Max}\mathcal{F}$ ($\operatorname{Min}\mathcal{F}$, $\operatorname{Med}\mathcal{F}$, resp.) vermöge $f \in \mathcal{F}$, wobei f polynomiell längenbeschränkt ist, so ist auch klarerweise h polynomiell längenbeschränkt.

Aus $\mathrm{id} \in \mathcal{F}$ folgt mit Lemma 5.6 direkt $\mathrm{id} \in \operatorname{Max}\mathcal{F}$ (bzw. $\operatorname{Min}\mathcal{F}$, $\operatorname{Med}\mathcal{F}$).

Sei nun $h \in \operatorname{Max}\mathcal{F}$, $h(x) = \max_{y \leq g(x)} f(x,y)$ for $f \in \mathcal{F}, g \in \mathrm{FP}$, und sei $g' \in \mathrm{FP}$. Dann gilt:

$$h \circ g'(x) = \max_{y \leq g(g'(x))} f(g'(x), y),$$

also $h \circ g' \in \operatorname{Max}\mathcal{F}$, denn $\lambda xy.f(g'(x),y) \in \mathcal{F}$ und $g \circ g' \in \mathrm{FP}$. Ein analoges Argument gilt für $\operatorname{Min}\mathcal{F}$ und $\operatorname{Med}\mathcal{F}$. Weiterhin gilt:

$$h(x) + g'(x) = \max_{y \leq g(x)} f(x,y) + g'(x) = \max_{y \leq g(x)} (f(x,y) + g'(x)),$$

also $h + g' \in \operatorname{Max}\mathcal{F}$, denn $\lambda xy.f(x,y) + g'(x) \in \mathcal{F}$. Ein analoges Argument gilt für $\operatorname{Min}\mathcal{F}$ und $\operatorname{Med}\mathcal{F}$. Multiplikation mit FP_+-Funktionen wird ebenfalls analog behandelt. Weiterhin gilt:

$$\max\{h(x), g'(x)\} = \max_{y \leq g(x)} \max\{f(x,y), g'(x)\}$$

und

$$\min\{h(x), g'(x)\} = \max_{y \leq g(x)} \min\{f(x,y), g'(x)\},$$

also $\max(f, g') \in \operatorname{Max}\mathcal{F}$, $\min(f, g') \in \operatorname{Max}\mathcal{F}$, denn $\lambda xy.\max\{f(x,y), g'(x)\} \in \mathcal{F}$ und $\lambda xy.\min\{f(x,y), g'(x)\} \in \mathcal{F}$. Ein analoges Argument gilt für $\operatorname{Min}\mathcal{F}$ und $\operatorname{Med}\mathcal{F}$.

Seien nun $h_1, h_2 \in \operatorname{Max}\mathcal{F}$, $h_i(x) = \max_{y \leq g_i(x)} f_i(x,y)$, wobei $f_i \in \mathcal{F}, g_i \in \mathrm{FP}$ ($i \in \{1,2\}$), und sei $A \in \mathrm{P}$. Wegen Lemma 5.5, können wir o.B.d.A. annehmen, daß $g_1 = g_2$. Sei

$$h(x) =_{\mathrm{def}} \begin{cases} h_1(x), & \text{falls } x \in A; \\ h_2(x), & \text{sonst.} \end{cases}$$

Dann gilt:

$$h(x) = \max_{y \leq g_1(x)} \begin{cases} f_1(x,y), & \text{falls } x \in A; \\ f_2(x,y), & \text{sonst.} \end{cases}$$

Also ist $h \in \operatorname{Max}\mathcal{F}$. Ein analoges Argument gilt für $\operatorname{Min}\mathcal{F}$ und $\operatorname{Med}\mathcal{F}$.

Wir wenden uns nun dem aufwendigsten Teil des Beweises zu, nämlich Abschluß unter Tupelbildung.

Sei $h \in \mathrm{Max}\,\mathcal{F}$, $g, g' \in \mathrm{FP}_+$, so daß $h(x,u) \in [g'(x)]$ für $u \in [g(x)]$. Sei $h(x,u) = \max_{y<g_1(x,u)} f(x,u,y)$ für $f \in \mathcal{F}$, $g_1 \in \mathrm{FP}$.

Sei $g_2 \in \mathrm{FP}$, so daß $g_1(x,u) \leq g_2(x)$ für $u \in [g(x)]$. Aus Lemma 5.5 folgt die Existenz einer Funktion $f_1 \in \mathcal{F}$, so daß $h(x,u) = \max_{y<g_2(x)} f_1(x,u,y)$ für $u \in [g(x)]$.

Definiere $f_2(x,u,y) =_{\mathrm{def}} \max\{-g'(x)+1, \min\{f_1(x,u,y), g'(x)\}\}$. Dann gilt $h(x,u) = \max_{y<g_2(x)} f_2(x,u,y)$ und $f_2(x,u,y) \in [g'(x)]$ für alle y und für $u \in [g(x)]$.

Definiere $f_3(x,z) =_{\mathrm{def}} f_2(x, z \div g_2(x), z \bmod g_2(x))$; sicherlich ist $f_3 \in \mathcal{F}$. Dann gilt aber für $u \in [g(x)]$ und $y < g_2(x)$, daß $f_3(x, u \cdot g_2(x) + y) = f_2(x,u,y)$. Für $z \in [g(x) \cdot g_2(x)]$ ist offensichtlich $z \div g_2(x) \in [g(x)]$, also gilt: $f_3(x,z) \in [g'(x)]$.

Nach Voraussetzung ist $\mathcal{F}$ abgeschlossen unter Tupelbildung. Also existieren $f_4 \in \mathcal{F}$, $\hat{g} \in \mathrm{FP}$, und r, so daß $r(x,z) \in [\hat{g}(x)]$ für alle y und $u \in [g(x)]$; und es gilt:

$$\begin{aligned} & f_4(x, \langle u_1 g_2(x) + y_1, \ldots, u_m g_2(x) + y_m \rangle_{g(x)\cdot g_2(x)}) \\ & \quad = \langle r(x, u_1 g_2(x) + y_1), f_3(x, u_1 g_2(x) + y_1), \ldots, f_3(x, u_m g_2(x) + y_m) \rangle_{\hat{g}(x), g'(x)} \end{aligned}$$

für $u_1, \ldots, u_m \in [g(x)]$ und $y_1, \ldots, y_m < g_2(x)$.

Definiere

$$\begin{aligned} & f_5(x,y,U) =_{\mathrm{def}} \\ & \quad f_4(x, \langle [U, g(x), 1] g_2(x) + y_1, \ldots, [U, g(x), m[U, g(x)]] g_2(x) + y_m \rangle), \end{aligned}$$

wobei $y_1, y_2, \ldots$ die Ziffern von y in $g_2(x)$-ärer Darstellung sind. Dann folgt für $u_1, \ldots, u_m \in [g(x)]$, daß

$$f_5(x, y, \langle u_1, \ldots, u_m \rangle_{g(x)}) = f_4(x, \langle u_1 g_2(x) + y_1, \ldots, u_m g_2(x) + y_m \rangle),$$

Definiere schließlich $h'(x,U) =_{\mathrm{def}} \max_{y<g_2(x)^{m[U,g(x)]}} f_5(x,y,U)$.

Dann gilt für $u_1, \ldots, u_m \in [g(x)]$:

$$\begin{aligned} & h'(x, \langle u_1, \ldots, u_m \rangle_{g(x)}) \\ & \quad = \max_{y_1,\ldots,y_m < g_2(x)} \langle r(x, u_1 g_2(x) + y_1), f_2(x, u_1, y_1), \ldots, f_2(x, u_m, y_m) \rangle_{\hat{g}(x), g'(x)} \\ & \quad = \langle s(x, u_1), \max_{y<g_2(x)} f_2(x, u_1, y), \ldots, \max_{y<g_2(x)} f_2(x, u_m, y) \rangle_{\hat{g}(x), g'(x)} \end{aligned}$$

wobei

$$s(x,u) =_{\mathrm{def}} \max\{\, r(x, u g_2(x) + y) \mid y < g_2(x) \wedge f_2(x,u,y) = \max_{z<g_2(x)} f_2(x,u,z) \,\};$$

offensichtlich ist $s(x,u) \in [\hat{g}(x)]$ für $u \in [g(x)]$.

Daraus folgt:

$$h'(x, \langle u_1, \ldots, u_m \rangle_{g(x)}) = \langle s(x, u_1), h(x, u_1), \ldots, h(x, u_m) \rangle_{\hat{g}(x), g'(x)}$$

für $u_1, \ldots, u_m \in [g(x)]$.

Ein analoger Beweis gilt für den Fall Min $\mathcal{F}$.

5.8 Bemerkung. Wir stellen zusätzlich folgendes fest: Ist die Funktion r konstant Null, so ist auch s konstant Null.

(Fortsetzung des Beweises:)

Im Falle Med $\mathcal{F}$ müssen wir gemäß den Überlegungen vor Definition 5.4 für Eindeutigkeit der auftretenden Werte sorgen. Das macht die Argumentation etwas aufwendiger; der prinzipielle Beweisverlauf ist jedoch wie oben im Falle von Max $\mathcal{F}$.

Sei $h \in \mathrm{Med}\,\mathcal{F}$, $g, g' \in \mathrm{FP}_+$ so daß $h(x, u) \in [g'(x)]$ für $u \in [g(x)]$. Sei $h(x, u) = \mathrm{med}_{y < g_1(x,u)} f(x, u, y)$ für $f \in \mathcal{F}$, $g_1 \in \mathrm{FP}$.

Sei $g_2 \in \mathrm{FP}$, so daß $g_1(x, u) \leq g_2(x)$ für $u \in [g(x)]$. Aus Lemma 5.5 folgt die Existenz einer Funktion $f_1 \in \mathcal{F}$, so daß $h(x, u) = \max_{y < g_2(x)} f_1(x, u, y)$ für $u \in [g(x)]$.

Definiere $f_2(x, u, y) =_{\mathrm{def}} \max\{-g'(x) + 1, \min\{f_1(x, u, y), g'(x)\}\}$. Dann gilt $h(x, u) = \mathrm{med}_{y < g_2(x)} f_2(x, u, y)$ und $f_2(x, u, y) \in [g'(x)]$ für alle y und $u \in [g(x)]$.

Definiere $f_2'(x, u, y) =_{\mathrm{def}} f_2(x, u, y) \cdot g_2(x) + y$. Dann ist $f_2' \in \mathcal{F}$, $f_2(x, u, \cdot)$ injektiv auf $\{0, \ldots, g_2(x) - 1\}$, und $f_2'(x, u, y) \in [g'(x) \cdot g_2(x)]$ für $u \in [g(x)]$. Definiere $g''(x) =_{\mathrm{def}} g'(x) \cdot g_2(x)$.

Definiere $f_3(x, z) =_{\mathrm{def}} f_2'(x, z \div g_2(x), z \bmod g_2(x))$; sicherlich ist$f_3 \in \mathcal{F}$. Dann gilt aber für $u \in [g(x)]$ und $y < g_2(x)$, daß $f_3(x, u \cdot g_2(x) + y) = f_2'(x, u, y)$. Für $z \in [g(x) \cdot g_2(x)]$ ist offensichtlich $z \div g_2(x) \in [g(x)]$, also gilt: $f_3(x, z) \in [g''(x)]$.

Nach Voraussetzung ist $\mathcal{F}$ abgeschlossen unter Tupelbildung. Also existieren $f_4 \in \mathcal{F}$, $\hat{g} \in \mathrm{FP}$, und r, so daß $r(x, z) \in [\hat{g}(x)]$ für alle y und $u \in [g(x)]$; und es gilt:

$$\begin{aligned} &f_4(x, \langle u_1 g_2(x) + y_1, \ldots, u_m g_2(x) + y_m \rangle_{g(x) \cdot g_2(x)}) \\ &\quad = \langle r(x, u_1 g_2(x) + y_1), f_3(x, u_1 g_2(x) + y_1), \ldots, f_3(x, u_m g_2(x) + y_m) \rangle_{\hat{g}(x), g''(x)} \end{aligned}$$

für $u_1, \ldots, u_m \in [g(x)]$ und $y_1, \ldots, y_m < g_2(x)$.

Definiere

$$\begin{aligned} &f_5(x, y, U) =_{\mathrm{def}} \\ &\quad f_4(x, \langle [U, g(x), 1] g_2(x) + y_1, \ldots, [U, g(x), m[U, g(x)]] g_2(x) + y_m \rangle), \end{aligned}$$

wobei $y_1, y_2, \ldots$ die Ziffern von y in $g_2(x)$-ärer Darstellung sind. Dann folgt für $u_1, \ldots, u_m \in [g(x)]$, daß

$$f_5(x, y, \langle u_1, \ldots, u_m \rangle_{g(x)}) = f_4(x, \langle u_1 g_2(x) + y_1, \ldots, u_m g_2(x) + y_m \rangle),$$

Definiere schließlich $h'(x, U) =_{\text{def}} \operatorname{med}_{y < g_2(x)^{m[U, g(x)]}} f_5(x, y, U)$.
Dann gilt für $u_1, \ldots, u_m \in [g(x)]$:

$$\begin{aligned}
&h'(x, \langle u_1, \ldots, u_m \rangle_{g(x)}) \\
&\quad = \operatorname*{med}_{y_1, \ldots, y_m < g_2(x)} \langle r(x, u_1 g_2(x) + y_1), f_2'(x, u_1, y_1), \ldots, f_2'(x, u_m, y_m) \rangle_{\hat{g}(x), g''(x)} \\
&\quad = \langle s(x, u_1), \operatorname*{med}_{y < g_2(x)} f_2'(x, u_1, y), \ldots, \operatorname*{med}_{y < g_2(x)} f_2'(x, u_m, y) \rangle_{\hat{g}(x), g''(x)}
\end{aligned}$$

wobei $s(x, u) =_{\text{def}} r(x, u g_2(x) + t(x, u))$ und $t(x, u) =_{\text{def}}$ das eindeutige y so daß $f_2'(x, u, y) = \operatorname{med}_{z < g_2(x)} f_2'(x, u, z)$. Die letzte Gleichheit und die Eindeutigkeit von y folgen aus der Injektivität von f_2'.

Daraus folgt:

$$\begin{aligned}
&h'(x, \langle u_1, \ldots, u_m \rangle_{g(x)}) \\
&\quad = \langle s(x, u_1), (\operatorname{med}_{y < g_2(x)} f_2(x, u_1, y)) \cdot g_2(x) + t(x, u_1), \\
&\qquad\qquad \ldots, (\operatorname{med}_{y < g_2(x)} f_2(x, u_m, y)) \cdot g_2(x) + t(x, u_m) \rangle_{\hat{g}(x), g''(x)} \\
&\quad = \langle s(x, u_1), h(x, u_1) \cdot g_2(x) + t(x, u_1), \\
&\qquad\qquad \ldots, h(x, u_m) \cdot g_2(x) + t(x, u_m) \rangle_{\hat{g}(x), g''(x)} \\
&\quad = \langle s'(x, u_1), h(x, u_1), \\
&\qquad\qquad \ldots, h(x, u_m) \rangle_{\hat{g}(x) \cdot g_2(x), g'(x)}.
\end{aligned}$$

für $u_1, \ldots, u_m \in [g(x)]$ und eine geeignet gewählte Funktion s'. □

5.3. Transformationen

Wir wenden uns nun dem systematischen Vergleich von Mengen- und Funktionenklassen zu. Dazu betrachten wir Operatoren, die Transformationen zwischen den Klassen durchführen. Unser Ziel ist es, zwei Operatoren zu finden, die bei der Transformation die Komplexität der Klasse möglichst beibehalten. Wir untersuchten bereits in Abschnitt 3.2 Operatoren, die von der Funktionenseite in die Mengenseite abbilden. Einer der dort betrachteten Operatoren war der Operator S. Er verfälscht die Komplexität bei der Transformation kaum, denn er ist in Polynomialzeit mit nur einer Frage an die betreffende Funktionenklasse zu berechnen, d.h. $\mathrm{S} \cdot \mathcal{F} \subseteq \mathrm{P}^{\mathcal{F}}[1]$. Dies trifft jedoch auch auf die anderen Operatoren aus Abschnitt 3.2 zu. S hat aber eine zusätzliche Eigenschaft, die ihn gegenüber den Operatoren U und X (und dem Operator $\oplus$ aus der Einleitung) auszeichnet, nämlich daß in der resultierenden Mengenklasse noch alle

Information über die Ausgangs-Funktionenklasse vorhanden ist. Es gilt nämlich offenbar $\mathcal{F} \subseteq \mathrm{FP}^{\mathrm{S}\mathcal{F}}$. Intuitiv hat die Klasse Med FP vergleichbare Komplexität wie die Mengenklasse PP. Ähnliches gilt für Max FP und NP (sowie Min FP und co-NP). Der Operator S führt nun tatsächlich die betreffenden Transformationen durch. In Satz 3.16 zeigten wir $\mathrm{S} \cdot \mathrm{Med\,FP} = \mathrm{PP}$ (und analoge Resultate für Max FP und Min FP werden wir später sehen).

Die Wahl des Operators für die Transformation in der umgekehrten Richtung liegt nicht so direkt auf der Hand. Sicherlich sollte auch er leicht zu berechnen sein und sich idealerweise – zumindest in den meisten interessanten Fällen – invers zu S verhalten. Es stellt sich heraus, daß diese Forderungen erfüllt werden von einem Operator, der einen bisher nicht benannten, aber dennoch einige Male in der Literatur [BuHa88, Wag90, AlWi90, Ogi91] benutzten monotonen Maximierungsoperator verallgemeinert.

5.9 Definition. Sei $\mathcal{K}$ eine Klasse von Mengen. Dann ist $f \in \mathrm{F} \cdot \mathcal{K}$ genau dann, wenn eine Menge $A \in \mathcal{K}$ und Funktionen $g_1, g_2 \in \mathrm{FP}$ existieren, so daß $(x, y+1) \in A \Rightarrow (x, y) \in A$ und

$$f(x) = \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x, y) \in A \,\},$$

falls diese Menge nichtleer ist, und $f(x) = g_1(x)$ sonst.

Offensichtlich ist F in Polynomialzeit mit Anfragen an die gegebene Mengenklasse berechenbar mittels binärer Suche. Zusammen mit den obigen Überlegungen zum Operator S erhalten wir damit folgende einfache Eigenschaften:

5.10 Beobachtung. *Sei $\mathcal{F}$ eine polynomiell-längenbeschränkte Funktionenklasse, abgeschlossen unter Eingabetransformationen, und sei $\mathcal{K}$ eine Mengenklasse, abgeschlossen unter many-one-Reduktionen. Dann gilt:*

1. $\mathrm{S} \cdot \mathcal{F} \subseteq \mathrm{P}^{\mathcal{F}}[1]$.
2. $\mathrm{F} \cdot \mathcal{K} \subseteq \mathrm{FP}^{\mathcal{K}}$.
3. $\mathrm{P}^{\mathrm{S} \cdot \mathcal{F}} = \mathrm{P}^{\mathcal{F}}$ *und* $\mathrm{FP}^{\mathrm{S} \cdot \mathcal{F}} = \mathrm{FP}^{\mathcal{F}}$
4. $\mathrm{P}^{\mathrm{F} \cdot \mathcal{K}} = \mathrm{P}^{\mathcal{K}}$ *und* $\mathrm{FP}^{\mathrm{F} \cdot \mathcal{K}} = \mathrm{FP}^{\mathcal{K}}$
5. $\mathrm{F} \cdot \mathrm{P} = \mathrm{FP}$
6. $\mathrm{S} \cdot \mathrm{FP} = \mathrm{P}$

Beweis. Vgl. die obige Diskussion. □

Wir möchten kurz auf eine andere, auf den ersten Blick natürlichere Möglichkeit, Funktionen in Mengen zu kodieren, eingehen. Wir denken dabei an die *Projektion* von Funktionen, d. h. für gegebene Funktion f an die Menge $\mathrm{proj}(f) =_{\mathrm{def}} \{(x,k) \mid f(x) \geq k\}$ (bzw. für eine Funktionenklasse $\mathcal{F}$ an $\mathrm{proj}(\mathcal{F}) =_{\mathrm{def}} \{\mathrm{proj}(f) \mid f \in \mathcal{F}\}$). Mengenklassen dieser Form sind jedoch im allgemeinen nicht unter many-one-Reduzierbarkeit abgeschlossen, ein schwerwiegender Nachteil (vgl. Kapitel 4). In den interessanten Fällen stellt sich jedoch heraus, daß der many-one-Abschluß von $\mathrm{proj}(\mathcal{F})$ genau die Klasse $\mathrm{S}\mathcal{F}$ ist. Es gilt nämlich:

5.11 Beobachtung. *Ist $\mathcal{F}$ eine Funktionenklasse mit der Eigenschaft $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$, so ist $\mathrm{S} \cdot \mathcal{F} = \mathcal{R}^{\mathrm{p}}_m(\mathrm{proj}(\mathcal{F}))$.*

Beweis. Sei $f \in \mathcal{F}$. Dann ist $\mathrm{proj}(f) \in \mathrm{S}\mathcal{F}$ direkt aufgrund der Definition. Offensichtlich ist unter den Voraussetzungen für $\mathcal{F}$ die Klasse $\mathrm{S}\mathcal{F}$ unter $\leq^{\mathrm{p}}_m$ abgeschlossen. Sei nun $A \in \mathrm{S}\mathcal{F}$, $x \in A \iff f(x) \geq g(x)$ für $f \in \mathcal{F}$ und $g \in \mathrm{FP}$. Dann ist $x \in A \iff (x, g(x)) \in \mathrm{proj}(f)$, also ist $A \in \mathcal{R}^{\mathrm{p}}_m(\mathrm{proj}(\mathcal{F}))$. □

Wir hatten oben gefordert, daß idealerweise S und F sich invers zueinander verhalten sollen. Gilt nämlich $\mathrm{S} \cdot \mathcal{F}_1 = \mathcal{K}_1$ und $\mathrm{S} \cdot \mathcal{F}_2 = \mathcal{K}_2$ sowie $\mathrm{F} \cdot \mathcal{K}_1 = \mathcal{F}_1$ und $\mathrm{F} \cdot \mathcal{K}_2 = \mathcal{F}_2$, so folgt $\mathcal{F}_1 \subseteq \mathcal{F}_2 \iff \mathcal{K}_1 \subseteq \mathcal{K}_2$, also insbesondere $\mathcal{F}_1 = \mathcal{F}_2 \iff \mathcal{K}_1 = \mathcal{K}_2$. Natürlich können wir nicht erwarten, daß S und F im Kontext beliebiger Klassen invers zueinander sind. S ist offensichtlich nicht injektiv (vgl. Satz 3.16). Außerdem ist die Berechnung von F zwar in Polynomialzeit möglich, aber es ist immerhin eine binäre Suche notwendig. Die Klasse $\mathrm{F}\mathcal{K}$ ist also eventuell von etwas höherer Komplexität als $\mathcal{K}$ selbst. Wir zeigen als nächstes, daß der Kompositionsoperator $\mathrm{S} \cdot \mathrm{F}$ tatsächlich ein Fixpunkt ist auf allen Mengenklassen, die im wesentlichen unter many-one-Reduktionen abgeschlossen sind. Die leicht höhere Komplexität von $\mathrm{F}\mathcal{K}$ kann also nicht genutzt werden, wenn nur durch den Flaschenhals des S-Operators ein Zugriff auf sie möglich ist. Auf der anderen seite können wir für allgemeines $\mathcal{F}$ die Komplexität von $\mathrm{FS} \cdot \mathcal{F}$ begrenzen, aber wir können nicht generell beweisen (und auch nicht erwarten), daß $\mathrm{F} \cdot \mathrm{S}$ ein Fixpunkt auf allen Funktionenklassen ist, die nur ähnlich schwache Voraussetzungen erfüllen wie die Ausgangs-Mengenklassen im Falle $\mathrm{S} \cdot \mathrm{F}$.

5.12 Satz.

1. *Ist $\mathcal{K}$ eine Mengenklasse, die P umfaßt und unter $\leq^{\mathrm{p}}_m$ abgeschlossen ist, so ist*
$$\mathrm{S} \cdot \mathrm{F} \cdot \mathcal{K} = \mathcal{K}.$$

2. *Ist $\mathcal{F}$ eine Funktionenklasse, die unter Eingabetransformationen abgeschlossen ist, so ist*
$$\mathcal{F} \subseteq \mathcal{F} - \mathrm{FP} \subseteq \mathrm{FS} \cdot \mathcal{F} = \mathrm{FS}(\mathcal{F} - \mathrm{FP}) = \mathrm{FS} \cdot \mathcal{F} - \mathrm{FP} \subseteq \mathrm{FP}^{\mathcal{F}}.$$

3. FS *ist ein Hüllenoperator für alle PFOs $\mathcal{F}$.*

Beweis.

1. Sei $A \in \mathrm{SF} \cdot \mathcal{K}$, $x \in A \iff f(x) \geq g(x)$, wobei $f \in \mathrm{F} \cdot \mathcal{K}$, $g \in \mathrm{FP}$. Dann gilt:
$$x \in A \iff \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in B \,\} \geq g(x)$$
für Funktionen $g_1, g_2 \in \mathrm{FP}$ und eine Menge $B \in \mathcal{K}$, $B \subseteq \mathbb{Z}^k$ für ein $k \in \mathbb{N}$. Also ist $x \in A \iff g_1(x) \leq g(x) \leq g_2(x) \wedge (x, g(x)) \in B$.
   (a) Ist $B = \mathbb{Z}^k$, so ist $x \in A \iff g_1(x) \leq g(x) \leq g_2(x)$. Also ist $A \in \mathrm{P}$ und damit in $\mathcal{K}$.
   (b) Ist $B \neq \mathbb{Z}^k$, so gibt es ein Paar $(x_0, y_0) \notin B$. Definiere
$$g''(x) = \begin{cases} (x, g(x)), & \text{falls } g_1(x) \leq g(x) \leq g_2(x) \\ (x_0, y_0), & \text{sonst.} \end{cases}$$
   Dann ist $g'' \in \mathrm{FP}$ und $x \in A \iff g''(x) \in B$. Also ist $A \in \mathcal{K}$.

   Sei nun umgekehrt $A \in \mathcal{K}$, $A \subseteq \mathbb{Z}^k$ für ein $k \in \mathbb{N}$. Definiere $A' = A \times \{1\} \cup \mathbb{Z}^k \times \{0\}$. Unter den Voraussetzungen des Satzes ist $A' \in \mathcal{K}$. Weiterhin gilt: $c_A(x) = \max\{\, y \mid 0 \leq y \leq 1 \wedge (x,y) \in A' \,\}$, also $c_A \in \mathrm{F} \cdot \mathcal{K}$. Da jedoch $x \in A \iff c_A(x) \geq 1$, folgt $A \in \mathrm{SF} \cdot \mathcal{K}$.

2. Sei $f \in \mathcal{F}$, $g \in \mathrm{FP}$. Seien $g', g'' \in \mathrm{FP}$ mit $g' < f < g''$. Dann gilt:
$$\begin{aligned} & f(x) - g(x) \\ & \quad = \max\{\, y \mid g'(x) - g(x) \leq y \leq g''(x) - g(x) \wedge f(x) - g(x) \geq y \,\} \\ & \quad = \max\{\, y \mid g'(x) - g(x) \leq y \leq g''(x) - g(x) \wedge f(x) \geq g(x) + y \,\} \end{aligned}$$
Also ist $f - g \in \mathrm{FS} \cdot \mathcal{F}$, und damit ist gezeigt: $\mathcal{F} - \mathrm{FP} \subseteq \mathrm{FS} \cdot \mathcal{F}$. Der Beweis von $\mathrm{FS}\mathcal{F} - \mathrm{FP} = \mathrm{FS}\mathcal{F}$ verläuft analog. $\mathrm{S}\mathcal{F} = \mathrm{S}(\mathcal{F} - \mathrm{FP})$ für alle Funktionenklassen ist offensichtlich.

3. Einbettung: $\mathcal{F} \subseteq \mathrm{FS}\mathcal{F}$ folgt aus Punkt 2.
   Monotonie: $\mathcal{F} \subseteq \mathcal{F}' \Rightarrow \mathrm{FS}\mathcal{F} \subseteq \mathrm{FS}\mathcal{F}'$ ist trivial.
   Abgeschlossenheit: $\mathrm{FS} \cdot \mathrm{FS} \cdot \mathcal{F} = \mathrm{FS} \cdot \mathcal{F}$ folgt aus Punkt 1, denn ist $\mathcal{F}$ eine PFO, so ist $\mathrm{S}\mathcal{F}$ abgeschlossen under $\leq_m^{\mathrm{p}}$ und umfaßt die Klasse P.

□

Damit $\mathcal{F}$ ein Fixpunkt von FS ist, müssen offensichtlich nichttriviale Abschlußeigenschaften von $\mathcal{F}$ gegeben sein. Wir definieren nun einen Operator BS, der binäre Suche unter den Werten einer monoton-fallenden Funktion formalisiert, und zeigen, daß er äquivalent zum Operator FS ist. Funktionenklassen $\mathcal{F}$ sind also genau dann Fixpunkte von FS, wenn sie abgeschlossen sind unter binärer Suche.

5.13 Definition. Sei $\mathcal{F}$ eine Funktionenklasse. Dann ist $f \in \mathrm{BS} \cdot \mathcal{F}$ genau dann, wenn Funktionen $f \in \mathcal{F}$ und $g, g_1, g_2 \in \mathrm{FP}$ existieren, so daß $f(x,y) \geq f(x,y+1)$ und

$$h(x) = \begin{cases} \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge f(x,y) \geq g(x)\,\}, & \text{falls } \{\ldots\} \neq \emptyset \\ g_1(x), & \text{sonst.} \end{cases}$$

5.14 Satz. *Ist $\mathcal{F}$ eine PFO, so ist* $\mathrm{FS} \cdot \mathcal{F} = \mathrm{BS} \cdot \mathcal{F}$.

Beweis. $\mathrm{BS} \cdot \mathcal{F} \subseteq \mathrm{FS} \cdot \mathcal{F}$ ist trivial.

Sei nun $h \in \mathrm{FS} \cdot \mathcal{F}$ vermöge $f \in \mathcal{F}$, $g, g_1, g_2 \in \mathrm{FP}$, wobei $f(x,y+1) \geq g(x,y+1)$ impliziert, daß $f(x,y) \geq g(x,y)$, und $h(x) = \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge f(x,y) \geq g(x,y)\,\}$ Aufgrund der PFO-Eigenschaften können wir oBdA annehmen, daß diese Menge nicht leer ist.

Definiere $f'(x,y) =_{\mathrm{def}} \max\{g(x,y) - 1, \min\{f(x,y), g(x,y)\}\}$. Dann ist $f' \in \mathcal{F}$ und es gilt:

$$f'(x,y) = \begin{cases} g(x,y), & \text{falls } f(x,y) \geq g(x,y) \\ g(x,y) - 1, & \text{falls } f(x,y) < g(x,y) \end{cases}$$

Sei $g' \in \mathrm{FP}$, so daß $g(x,y) < g'(x)$ für $g_1(x) \leq y \leq g_2(x)$. Definiere $f''(x,y) =_{\mathrm{def}} f'(x,y) + (g'(x) - g(x,y))$. Dann ist $f'' \in \mathcal{F}$ und es gilt:

$$f''(x,y) = \begin{cases} g'(x), & \text{falls } f(x,y) \geq g(x,y) \\ g'(x) - 1, & \text{falls } f(x,y) < g(x,y) \end{cases}$$

Offensichtlich gilt nun $f''(x,y) \geq f''(x,y+1)$ und $h(x) = \max\{\, y \mid g_1(x) \leq g_2(x) \wedge f''(x,y) \geq g'(x)\,\}$. □

Wir werden in den nächsten Abschnitten sehen, daß erstaunlich viele natürliche Funktionenklassen unter binärer Suche, wie eben definiert, abgeschlossen sind.

Die Inklusion $\mathcal{F} \subseteq \mathrm{FS}\mathcal{F}$ wird also zur Gleichheit, wenn $\mathcal{F}$ unter binärer Suche abgeschlossen ist. Wir wenden uns als nächstes der Inklusion $\mathrm{FS}\mathcal{F} \subseteq \mathrm{FP}^{\mathcal{F}}$ zu. Es zeigt sich, daß erstaunlicherweise jede Funktion aus $\mathrm{FP}^{\mathcal{F}}$ mit nur einer Frage an eine $\mathrm{FS}\cdot\mathcal{F}$-Funktion berechnet werden kann und sogar bereits als Differenz zweier $\mathrm{FS}\mathcal{F}$-Funktionen geschrieben werden kann.

5.15 Satz. *Ist die Funktionenklasse $\mathcal{F}$ eine PFO, so gilt:*

$$\mathrm{FP}^{\mathcal{F}} = (\mathrm{FS}\cdot\mathcal{F} \bmod 2\mathrm{FP}) - \mathrm{FP} = \mathrm{FS}\cdot\mathcal{F} - \mathrm{FS}\cdot\mathcal{F}.$$

Beweis. Sei $f \in \mathcal{F}$ und $h \in \mathrm{FP}^f$ vermöge der Turing-Maschine M. OBdA existieren $s, g, g' \in \mathrm{FP}$, so daß $h(x) \in [g(x)]$, M stellt bei Eingabe x genau $s(x)$ Fragen aus dem Bereich $[g(x)]$, und $f'(y) \in [g'(x)]$ für alle $y \in [g(x)]$. Da $\mathcal{F}$ unter Tupelbildung abgeschlossen ist, existieren $f' \in \mathcal{F}$, $\hat{g} \in \mathrm{FP}$, und r, so daß

$$f'(x, \langle u_1, \ldots, u_m\rangle_{g(x)}) = \langle r(x, u_1), f(u_1), \ldots, r(x, u_m), f(u_m)\rangle_{\hat{g}(x), g'(x)}.$$

Für $v_1, \ldots, v_{s(x)} \in [g'(x)]$ schreiben wir abkürzend $\bar{v} = \langle v_1, \ldots, v_{s(x)}\rangle_{g'(x)}$. Betrachte nun eine Berechnung von M bei Eingabe x, bei der jedoch $v_1, \ldots, v_{s(x)}$ anstelle der Orakelantworten eingesetzt werden. Sei

$$\mathrm{output}(x, \bar{v})$$

die Ausgabe von M bei der so definierten Berechnung.

Definiere

$$\mathrm{queries}(x, \bar{v}) =_{\mathrm{def}} \langle q_{s(x)}, \ldots, q_1\rangle_{g(x)},$$

wobei q_i die i-te Frage in dieser Berechnung ist. Es ist offensichtlich, daß $\mathrm{output}, \mathrm{queries} \in \mathrm{FP}$.

Definiere

$$\mathrm{path}(x, \bar{v}) =_{\mathrm{def}} \langle \mathrm{output}(x, \bar{v}), f'(x, \mathrm{queries}(x, \bar{v}))\rangle_{g(x)}.$$

Dann ist $\mathrm{path} \in \mathcal{F}$. Definiere eine zweistellige Funktion $\mathrm{answers} \in \mathrm{FP}$, so daß

$$\mathrm{answers}(x, \langle u, \langle r_{s(x)}, v_{s(x)}, \ldots, r_1, v_1\rangle_{\hat{g}(x), g'(x)}\rangle_{g(x)} = \bar{v}$$

für $v_1, \ldots, v_{s(x)} \in [g'(x)]$, $r_1, \ldots, r_{s(x)} \in [\hat{g}(x)]$ und $u \in [g(x)]$. Definiere

$$\mathrm{better\_path}(x, z) =_{\mathrm{def}} \mathrm{path}(x, \mathrm{answers}(x, z)).$$

Offensichtlich ist $\mathrm{better\_path} \in \mathcal{F}$.

Seien nun $q_1, \ldots, q_{s(x)}$ und $v_1, \ldots, v_{s(x)}$ die Folgen der korrekten Fragen und Antworten der Berechnung von M bei Eingabe x mit Orakel f. Das heißt also $f(q_i) = v_i$, $\mathrm{queries}(x, \bar{v}) = \langle q_{s(x)}, \ldots, q_1\rangle_{g(x)}$, und $\mathrm{output}(x, \bar{v}) = h(x)$. Sei $r_i =_{\mathrm{def}} r(x, q_i)$; dann gilt:

$$z =_{\mathrm{def}} \mathrm{path}(x, \bar{v}) = \langle h(x), \langle r_{s(x)}, v_{s(x)}, \ldots, r_1, v_1\rangle_{\hat{g}(x), g'(x)}\rangle_{g(x)},$$

answers$(x, z) = \bar{v}$ und better_path$(x, z) = z$. Definiere correct_path$(x) =_{\text{def}} z$.

Seien nun $v'_1, \ldots, v'_{s(x)} \in [g'(x)]$, $r'_1, \ldots, r'_{s(x)} \in [\hat{g}(x)]$ und $u' \in [g(x)]$ beliebig. Definiere

$$\begin{aligned} \bar{v}' &=_{\text{def}} \langle v'_1, \ldots, v'_{s(x)} \rangle_{g'(x)} \\ z' &=_{\text{def}} \langle u', \langle r'_{s(x)}, v'_{s(x)}, \ldots, r'_1, v'_1 \rangle_{\hat{g}(x), g'(x)} \rangle_{g(x)} \end{aligned}$$

Definiere $q''_1, \ldots, q''_{s(x)}$, so daß queries$(x, \bar{v}') = \langle q''_{s(x)}, \ldots, q''_1 \rangle_{g(x)}$, und definiere $u'' =_{\text{def}}$ output$(x, \bar{v}')$, $v''_i =_{\text{def}} f(q''_i)$, and $r''_i =_{\text{def}} r(x, q''_i)$. Sicherlich ist dann answers$(x, z') = \bar{v}'$ und

$$z'' =_{\text{def}} \text{better\_path}(x, z') = \langle u'', \langle r''_{s(x)}, v''_{s(x)}, \ldots, r''_1, v''_1 \rangle_{\hat{g}(x), g'(x)} \rangle_{g(x)}.$$

Ist $z' < z$, so existiert ein größter Wert $i \in \{0, 1, \ldots, s(x)\}$, für den $v'_j = v_j$ für $j = 1, \ldots, i$ und $r'_j = r_j$ für $j = 1, \ldots, i-1$.

Fall 1, $i < s(x)$: Wegen $v'_j = v_j$ für $j = 1, \ldots, i$, ist $q''_j = q_j$ für $j = 1, \ldots, i+1$. Also ist $v''_j = f(q''_j) = f(q_j) = v_j$ for $j = 1, \ldots, i+1$. Aus der Wahl von i und der Tatsache $z' < z$ ergibt sich $r'_i < r_i = r''_i$ oder ($r'_i = r_i = r''_i$ und $v'_{i+1} < v_{i+1} = v''_{i+1}$). Daraus folgt: $z' < z''$.

Fall 2, $i = s(x)$: Dann ist $u'' =$ output$(x, \bar{v}') =$ output$(x, \bar{v}) = h(x)$ und $v''_j = f(q''_j) = f(q_j) = v_j$ für $j = i, \ldots, s(x)$. Wegen $z' < z$ ergibt sich $r'_{s(x)} < r_{s(x)} = r''_{s(x)}$ oder ($r'_{s(x)} = r_{s(x)} = r''_{s(x)}$ und $u' < h(x) = u''$). Daraus folgt: $z' < z''$.

Ist $z' > z$, so erhalten wir durch eine analoge Argumentation $z' > z''$. Insgesamt gilt also:

$$\text{better\_path}(x, z') \begin{cases} = z', & \text{falls } z' = \text{correct\_path}(x) \\ > z', & \text{falls } z' < \text{correct\_path}(x) \\ < z', & \text{falls } z' > \text{correct\_path}(x) \end{cases}$$

Definiere

$$A =_{\text{def}} \{ (x, z') \mid \text{better\_path}(x, z') \geq z' \} = \{ (x, z') \mid z' \leq \text{correct\_path}(x) \};$$

dann ist $A \in \mathrm{S}\mathcal{F}$, $(x, z'+1) \in A \Rightarrow (x, z') \in A$ und

$$\text{correct\_path}(x) = \max\{ z' \mid 0 \leq z' \leq \bar{g}(x) \wedge (x, z') \in A \}$$

für eine geeignete FP-Funktion $\bar{g}$. Also ist correct_path $\in \mathrm{FS} \cdot \mathcal{F}$.

Weiterhin gibt es ein $t \geq 0$, für das correct_path$(x) = \langle h(x), t \rangle_{g(x)} = h(x) + g(x) + 2 \cdot g(x)(t + g(x)) - 1$. Daraus folgt: $h(x) =$ correct_path$(x) \bmod 2g(x) - g(x) + 1$.

Definieren wir weiterhin correct_path′ analog zu correct_path mit dem einzigen Unterschied, daß wir nun als Ausgabefunktion konstant die Null verwenden, ergibt sich:

$$h(x) = \text{correct\_path}(x) - \text{correct\_path}'(x).$$

□

5.4. Abschlußeigenschaften

Wir haben in Kapitel 4 ein vernünftiges Axiomensystem für Mengenklassen unter dem Namen APK eingeführt. Das gleiche haben wir im Abschnitt 5.2 dieses Kapitels für eine bestimmte Kategorie von Funktionenklassen getan. Wir ließen uns in Definition 5.4 teilweise leiten von Analogieüberlegungen zur Definition 4.1. Wir werden in diesem Abschnitt sehen, daß die geforderten Abschlußeigenschaften tatsächlich unter den Operatoren S und F ineinander fast „übersetzt“ werden. Leider ist die Analogie zwischen APK und PFO nicht vollkommen. Eine APK entspricht auf der Funktionenseite einer strengen Form von PFO.

5.16 Definition. Eine Funktionenklasse $\mathcal{F}$ ist eine *streng p-fundierte Klasse von Optimierungsfunktionen (SPFO)*, falls gilt:

1. $\mathcal{F}$ ist eine PFO.

2. Für $f \in \mathcal{F}$, $g, g' \in \mathrm{FP}_+$, wobei $f(x,u) \in [g'(x)]$ für $u \in [g(x)]$, existiert $h \in \mathcal{F}$, so daß für alle $m \in \mathbb{N}$, $u_1, \ldots, u_m \in [g(x)]$ gilt:

   $$h(x, \langle u_1, \ldots, u_m \rangle_{g(x)}) = \langle f(x,u_1), \ldots, f(x,u_m) \rangle_{g'(x)}.$$

   (*Starker Abschluß unter Tupelbildung*)

Die zweite Bedingung oben verschärft also den Punkt 6 aus Definition 5.4. Die Überlegungen vor Definition 5.4 deuteten bereits darauf hin, daß Max- und Min-Klassen diese starke Abschlußeigenschaft besitzen.

5.17 Satz.

1. FP *ist eine SPFO.*

2. Ist $\mathcal{F}$ eine SPFO, so sind auch $\mathrm{Max}\,\mathcal{F}$ *und* $\mathrm{Min}\,\mathcal{F}$ *SPFOs.*

Beweis. Folgt aus Bemerkung 5.8. □

Die Diskussion vor Definition 5.4 deutete an, warum wir in die Aussage von Satz 5.17 die Med-Klassen nicht mit aufnehmen können. Es wird sich jedoch später zeigen, daß unter leichten zusätzlichen Voraussetzungen an eine PFO $\mathcal{F}$ folgt, daß die Klassen $\mathrm{Max}\,\mathcal{F}$, $\mathrm{Min}\,\mathcal{F}$ sowie $\mathrm{FS}\cdot\mathrm{Med}\,\mathcal{F}$ SPFOs sind.

Tabelle 5.1 faßt die bisher nur intuitiv vorhandenen Beziehungen zwischen APKs und SPFOs formal. Jede Zeile der Tabelle ist folgendermaßen zu interpretieren: Gilt $\boxed{\mathrm{A}}$ und ist $\mathcal{K} = \mathrm{S}\cdot\mathcal{F}$, so gilt $\boxed{\mathrm{B}}$. Gilt $\boxed{\mathrm{B}}$ und ist $\mathcal{F} = \mathrm{F}\cdot\mathcal{K}$, so gilt $\boxed{\mathrm{A}}$. Die folgenden Lemmata beweisen die nicht-trivialen Behauptungen der Tabelle.

	$\boxed{\mathrm{A}}$	$\boxed{\mathrm{B}}$
1	$\mathrm{FP} \subseteq \mathcal{F}$	$\mathrm{P} \subseteq \mathcal{K}$
2	$\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$	$\mathcal{K}$ abgeschlossen unter $\leq_m^{\mathrm{P}}$
3	$\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$ $\mathcal{F} + \mathrm{FP}_+ \subseteq \mathcal{F}, \mathcal{F} \cdot \mathrm{FP}_+ \subseteq \mathcal{F}$ $\mathcal{F}$ abgeschl. Fallunterscheidung	$\mathcal{K}$ abgeschlossen unter $\leq_m^{\mathrm{P}}$ $\mathcal{K}$ abgeschl. unter mark. Vereinigung
4	$\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}, \mathcal{F} + \mathrm{FP}_+ \subseteq \mathcal{F}$ $\min(\mathcal{F}, \mathcal{F}) \subseteq \mathcal{F}$	$\mathcal{K}$ abgeschlossen unter $\leq_m^{\mathrm{P}}$ $\mathcal{K}$ abgeschlossen unter Schnitt
5	$\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}, \mathcal{F} + \mathrm{FP}_+ \subseteq \mathcal{F}$ $\max(\mathcal{F}, \mathcal{F}) \subseteq \mathcal{F}$	$\mathcal{K}$ abgeschlossen unter $\leq_m^{\mathrm{P}}$ $\mathcal{K}$ abgeschlossen unter Vereinigung
6	$\mathrm{FP} \subseteq \mathcal{F}$ $\min(\mathcal{F}, \mathrm{FP}) \subseteq \mathcal{F}, \max(\mathcal{F}, \mathrm{FP}) \subseteq \mathcal{F}$ $\mathcal{F}$ str. abgeschl. Tupelbildung	$\mathrm{P} \subseteq \mathcal{K}$ $\mathcal{K}$ abgeschl. unter $\leq_{ctt}^{\mathrm{P}}$ und $\leq_{dtt}^{\mathrm{P}}$
7	$\mathcal{F} = -\mathcal{F}$	$\mathcal{K}$ abgeschl. unter Komplement

Tabelle 5.1: Übertragungen von Abschlußeigenschaften

5.18 Lemma.

1. *Sei die Mengenklasse $\mathcal{K}$ abgeschlossen unter $\leq_m^{\mathrm{P}}$. Dann gilt:*
   (a) $\mathrm{F}\cdot\mathcal{K} = \mathrm{F}\cdot\mathcal{K} - \mathrm{FP}$.
   (b) $\mathrm{F}\cdot\text{co-}\mathcal{K} = -\mathrm{F}\mathcal{K}$.
2. *Sei $\mathcal{F}$ eine Funktionenklasse. Dann gilt:* $\mathrm{S}(-\mathcal{F}) = \text{co-S}\mathcal{F}$.
3. *Ist $\mathcal{F}$ eine Funktionenklasse, die unter Eingabetransformationen abgeschlossen ist, so gilt:* $\mathrm{FS}(-\mathcal{F}) = -\mathrm{FS}\cdot\mathcal{F}$.

Beweis.

1. (a) Sei $f(x) = \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x,y) \in A \,\}$, $A \in \mathcal{K}$, $g_1, g_2 \in \mathrm{FP}$, wobei $(x, y+1) \in A$ impliziert, daß $(x,y) \in A$. Sei

$g \in \mathrm{FP}$. Dann gilt:

$$f(x) - g(x) = \\ \max\{\, y \mid g_1(x) - g(x) \leq y \leq g_2(x) - g(x) \wedge (x, y + g(x)) \in A \,\}.$$

Definiere $A' \leq_m^{\mathrm{p}} A$ folgendermaßen:

$$(x,y) \in A' \iff (x, y + g(x)) \in A.$$

Daraus folgt: $f - g \in \mathrm{F}\mathcal{K}$.

(b) Sei $f \in \mathrm{F}\cdot\text{co-}\mathcal{K}$, $f(x) = \max\{\, y \mid g_1(x) \leq y < g_2(x) \wedge (x,y) \in A \,\}$, $A \in \text{co-}\mathcal{K}$, $g_1, g_2 \in \mathrm{FP}$, wobei $(x, y{+}1) \in A$ impliziert, daß $(x,y) \in A$. Definiere

$$f'(x) =_{\text{def}} \max\{\, y \mid 0 \leq y < g_2(x) - g_1(x) \wedge (x, g_2(x) - y) \in \overline{A} \,\}.$$

Dann gilt: $(x,y) \in \overline{A} \Rightarrow (x, y+1) \in \overline{A}$. Definiere $A' \leq_m^{\mathrm{p}} A$ via

$$(x,y) \in A' \iff (x, g_2(x) - y) \in \overline{A}.$$

Daraus folgt: $f' \in \mathrm{F}\mathcal{K}$. Es gilt jedoch offensichtlich $f(x) + f'(x) + 1 = g_2(x)$. Also ergibt sich $\mathrm{F}\cdot\text{co-}\mathcal{K} \subseteq -\mathrm{F}\mathcal{K} + \mathrm{FP} = -\mathrm{F}\mathcal{K}$. $\mathrm{F}\mathcal{K} \subseteq -\mathrm{F}\cdot\text{co-}\mathcal{K}$ zeigt man analog.

2. Sei $A \in \mathrm{S}(-\mathcal{F})$, $x \in A \iff -f(x) \geq g(x)$ für $f \in \mathcal{F}$ and $g \in \mathrm{FP}$. Dann ist

$$x \in \overline{A} \iff -f(x) < g(x) \iff f(x) > -g(x) \iff f(x) \geq -g(x) + 1.$$

Also folgt $\overline{A} \in \mathrm{S}\mathcal{F}$, und daher $A \in \text{co-}\mathrm{S}\mathcal{F}$. Es gilt also: $\mathrm{S}(-\mathcal{F}) \subseteq \text{co-}\mathrm{S}\mathcal{F}$. Umgekehrt gilt: $\text{co-}\mathrm{S}\mathcal{F} \subseteq \text{co-}\mathrm{S}(-(-\mathcal{F})) \subseteq \text{co-co-}\mathrm{S}(-\mathcal{F}) \subseteq \mathrm{S}(-\mathcal{F})$.

3. Folgt direkt aus den ersten beiden Behauptungen.

□

5.19 Lemma.

1. *Ist $\mathcal{F}$ eine Funktionenklasse, die abgeschlossen ist unter Eingabetransformationen und Definition durch Fallunterscheidung, so ist $\mathcal{K} =_{\text{def}} \mathrm{S}\cdot\mathcal{F}$ abgeschlossen unter markierter Vereinigung.*

2. *Ist $\mathcal{K}$ eine Mengenklasse, die abgeschlossen ist unter $\leq_m^{\mathrm{p}}$ und markierter Vereinigung, so ist $\mathcal{F} =_{\text{def}} \mathrm{F}\cdot\mathcal{K}$ abgeschlossen unter Definition durch Fallunterscheidung.*

Beweis.

1. Seien $A_1, A_2 \in \mathcal{K}$, $x \in A_i \iff f_i(x) \geq g_i(x)$ für $f_i \in \mathcal{F}$, $g_i \in \mathrm{FP}$ $(i = 1, 2)$. Sei $A = 0A_1 \cup 1A_2$.

   Definiere
$$f(x) = \begin{cases} f_1(z), & \text{falls } x = 0z; \\ f_2(z), & \text{falls } x = 1z. \end{cases}$$
$$g(x) = \begin{cases} g_1(z), & \text{falls } x = 0z; \\ g_2(z), & \text{falls } x = 1z. \end{cases}$$

   Offensichtlich gilt: $f \in \mathcal{F}$, $g \in \mathrm{FP}$ und $x \in A \iff f(x) \geq g(x)$. Also ist $A \in \mathcal{K}$.

2. Seien $f_1, f_2 \in \mathcal{F}$, $f_i(x) = \max\{\, y \mid g_{i,1}(x) \leq y \leq g_{i,2}(x) \wedge (x, y) \in B_i \,\}$ für $B_i \in \mathcal{K}$, $g_{i,1}, g_{i,2} \in \mathrm{FP}$ $(i = 1, 2)$. Sei $A \in \mathrm{P}$. Sei f definiert durch
$$f(x) =_{\mathrm{def}} \begin{cases} f_1(x), & \text{falls } x \in A; \\ f_2(x), & \text{sonst.} \end{cases}$$

   Definiere
$$B = \{\, (x, y) \mid (x \in A \wedge (x, y) \in B_1) \vee (x \notin A \wedge (x, y) \in B_2) \,\}.$$

   Dann ist $B \leq_m^{\mathrm{P}} 0B_1 \cup 1B_2$, also folgt: $B \in \mathcal{K}$. Definiere
$$g_j(x) = \begin{cases} g_{1,j}, & \text{falls } x \in A; \\ g_{2,j}, & \text{sonst.} \end{cases} \qquad (j = 1, 2)$$

   Dann sind $g_1, g_2 \in \mathrm{FP}$ und
$$f(x) = \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x, y) \in B \,\}.$$

   Also ist $f \in \mathcal{F}$.

□

5.20 Lemma.

1. *Ist $\mathcal{F}$ eine Funktionenklasse, die abgeschlossen ist unter Eingabetransformationen und min-max-Operationen mit* FP*-Funktionen und streng abgeschlossen ist unter Tupelbildung, so ist $\mathcal{K} =_{\mathrm{def}} \mathrm{S} \cdot \mathcal{F}$ abgeschlossen unter disjunktiven und konjunktiven Reduktionen.*

2. *Ist $\mathcal{K}$ eine Mengenklasse, die unter konjunktiven und disjunktiven Reduktionen abgeschlossen ist, so ist $\mathcal{F} =_{\mathrm{def}} \mathrm{F} \cdot \mathcal{K}$ streng abgeschlossen unter Tupelbildung.*

Beweis.

1. Sei $A \in \mathcal{K}$, $x \in A \iff f(x) \geq g(x)$ für Funktionen $f \in \mathcal{F}$, $g \in \mathrm{FP}$. Sei $x \in B \iff x_1 \in A \vee x_2 \in A \vee \cdots \vee x_m \in A$, wobei die Wörter $x_1, \ldots, x_m$ deterministisch in Polynomialzeit, gegeben x, berechnet werden können. Seien $g_1, g_2 \in \mathrm{FP}$, so daß $x_1, \ldots, x_m \in [g_1(x)]$ und $f(z), g(z) \in [g_2(x)]$ für alle $z \in [g_1(x)]$.

   Dann gilt:

$$\begin{aligned} x \in B &\iff f(x_1) \geq g(x_1) \vee \cdots \vee f(x_m) \geq g(x_m) \\ &\iff \max\{f(x_1), g(x_1) - 1\} > g(x_1) - 1 \vee \cdots \\ &\qquad\qquad \vee \max\{f(x_m), g(x_m) - 1\} > g(x_m) - 1 \\ &\iff \langle \max\{f(x_1), g(x_1) - 1\}, \ldots, \max\{f(x_m), g(x_m) - 1\} \rangle_{g_2(x)} \\ &\qquad\qquad > \langle g(x_1) - 1, \ldots, g(x_m) - 1 \rangle_{g_2(x)} \end{aligned}$$

   Sei nun $x \in B \iff x_1 \in A \wedge x_2 \in A \wedge \cdots \wedge x_m \in A$ wobei die Wörter $x_1, \ldots, x_m$ deterministisch in Polynomialzeit, gegeben x, berechnet werden können. Seien g_1, g_2 wie oben.

   Dann gilt:

$$\begin{aligned} x \in B &\iff f(x_1) \geq g(x_1) \wedge \cdots \wedge f(x_m) \geq g(x_m) \\ &\iff \min\{f(x_1), g(x_1)\} \geq g(x_1) \wedge \cdots \\ &\qquad\qquad \wedge \min\{f(x_m), g(x_m)\} \geq g(x_m) \\ &\iff \langle \min\{f(x_1), g(x_1)\}, \ldots, \min\{f(x_m), g(x_m)\} \rangle_{g_2(x)} \\ &\qquad\qquad \geq \langle g(x_1), \ldots, g(x_m) \rangle_{g_2(x)}. \end{aligned}$$

2. Sei $f \in \mathcal{F}$, $f(x) = \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x, y) \in A \,\}$ für $A \in \mathcal{K}$, $g_1, g_2 \in \mathrm{FP}$. Sei $\hat{f}(x, \langle u_1, \ldots, u_m \rangle_{g_3(x)}) = \langle f(u_1), \ldots, f(u_m) \rangle_{g_4(x)}$ für $g_3, g_4 \in \mathrm{FP}$. Zu zeigen ist $\hat{f} \in \mathcal{F}$.

   Definiere dazu folgende Menge $\hat{A}$:

$$(x, \langle u_1, \ldots, u_m \rangle_{g_3(x)}, \langle z_1, \ldots, z_m \rangle_{g_4(x)}) \in \hat{A}$$

   genau dann, wenn

   (a) für alle $i = 1, \ldots, m$ gilt, daß $(u_i, z_i) \in A$;
   oder

   (b) es gibt ein $i \in \{1, \ldots, m\}$, so daß $(u_i, z_i + 1) \in A$ und für alle $j = i + 1, \ldots, m$ gilt, daß $(u_j, z_j) \in A$.

   Offensichtlich ist $\hat{A}$ in $\mathcal{K}$.

   Da jedoch $\hat{f}(x, u)$ gleich dem maximalen z in einem geeigneten Bereich ist, für das $(x, u, z) \in \hat{A}$, folgt $\hat{f} \in \mathcal{F}$.

□

Aus den Einzelresultaten der Tabelle 5.1 ergeben sich folgende interessante Korollare:

5.21 Korollar.

1. *Ist $\mathcal{F}$ eine SPFO, so ist* $\mathrm{S} \cdot \mathcal{F}$ *eine APK.*
2. *Ist $\mathcal{K}$ eine APK, so ist* $\mathrm{F} \cdot \mathcal{K}$ *eine SPFO.*

5.22 Korollar. *Ist $\mathcal{F}$ eine SPFO, so ist auch* $\mathrm{F} \cdot \mathrm{S} \cdot \mathcal{F}$ *eine SPFO.*

Auf der Suche nach einer Entsprechung von Korollar 5.22 für PFOs führen wir folgenden Begriff ein:

Eine Mengenklasse hat die $\times$-Eigenschaft, falls für alle $B \in \mathcal{K}$ mit $(x, y+1) \in B \Rightarrow (x, y) \in B$ ein $B^* \in \mathcal{K}$ existiert, so daß gilt: Für alle $\langle u_1, \ldots, u_m \rangle$, $\langle z_1, \ldots, z_m \rangle$ mit $(u_i, z_i) \in B$ für $i = 1, \ldots, m$ existieren $y_1, \ldots, y_m$, so daß für alle $\bar{z} \leq \langle y_1, z_1, \ldots, y_m, z_m \rangle$ gilt: $(x, \langle u_1, \ldots, u_m \rangle, \bar{z}) \in B^*$.

Die $\times$-Eigenschaft ist eine direkte Übertragung des Abschlusses unter Tupelbildung auf die Mengenseite. Daher ist folgende Beobachtung evident:

5.23 Beobachtung.

1. *Ist $\mathcal{F}$ eine PFO, so hat* $\mathrm{proj}(\mathcal{F})$ *die $\times$-Eigenschaft.*
2. *Ist $\mathcal{K}$ eine Mengenklasse, die* P *umfaßt, unter many-one-Reduktionen und markierter Vereinigung abgeschlossen ist und die $\times$-Eigenschaft hat, so ist* $\mathrm{F} \cdot \mathcal{K}$ *eine PFO.*

Eine natürlicheres Pendant zu den PFO-Bedingungen scheint nicht zu existieren. Daher werden wir im folgenden die $\times$-Eigenschaft nicht weiter benutzen, sondern unsere Resultate etwas weniger allgemein, aber anschaulich, nur für APKs formulieren. Der Grund für uns, die $\times$-Eigenschaft hier aufzuführen, ist das folgende Korollar, das sich direkt aus Beobachtung 5.23 ergibt:

5.24 Korollar. *Ist $\mathcal{F}$ eine PFO, so ist auch* $\mathrm{F} \cdot \mathrm{S} \cdot \mathcal{F}$ *eine PFO.*

Mit Hilfe von Korollar 5.21 lassen sich nun Resultate von der Funktionenseite direkt auf die Mengenseite übertragen. Aus Satz 5.15 folgt direkt:

5.25 Korollar. *Ist $\mathcal{K}$ eine APK, so gilt:* $\mathrm{FP}^{\mathcal{K}} = \mathcal{F} \cdot \mathcal{K} - \mathcal{F} \cdot \mathcal{K}$.

5.26 Korollar. *Ist $\mathcal{K}$ eine APK, so gilt:* $\mathrm{P}^{\mathcal{K}} = \oplus\, \mathrm{F}\mathcal{K}$.

Korollar 5.26 verallgemeinert ein Resultat von Ogiwara [Ogi91]. Er benötigte die zusätzliche Voraussetzung $\mathcal{K} = \exists\mathcal{K}$ oder $\mathcal{K} = \forall\mathcal{K}$.

5.5. Beziehungen zu Mengenklassen

5.5.1. Beziehungen zwischen Operatoren

Wir werden in diesem Abschnitt sehen, daß die Konversionsoperatoren F und S eine enge Beziehung zwischen den funktionstheoretischen Operatoren Max, Min und Med aus Abschnitt 5.1 und den mengentheoretischen Operatoren $\exists$, $\forall$ und C etablieren. Die engsten Verbindungen ergeben sich für Max/$\exists$ und Min/$\forall$. Wenden wir auf eine Funktionenklasse $\mathcal{F}$ zunächst den Operator Max an und wechseln dann mit S zur Mengenseite über, so erhalten wir genau die Klasse, die zunächst die Anwendung des Konversionsoperators S und anschließend des mengentheoretischen Operators $\exists$ ergibt. Die Resultate aus Lemma 5.18 erlauben dann direkt eine ähnliche Aussage für Min und $\forall$.

5.27 Satz. *Sei $\mathcal{F}$ eine Funktionenklasse, für die $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$ und $\mathcal{F} + \mathrm{FP}_+ \subseteq \mathcal{F}$ gelten und sei $\mathcal{K}$ eine Mengenklasse, die unter $\leq_m^{\mathrm{p}}$ abgeschlossen ist und die Klasse* P *umfaßt. Dann gilt:*

1. $\mathrm{S} \cdot \mathrm{Max} \cdot \mathcal{F} = \exists \cdot \mathrm{S}\mathcal{F}$ *and* $\mathrm{F} \cdot \exists \cdot \mathcal{K} = \mathrm{Max} \cdot \mathrm{F}\mathcal{K}$.
2. $\mathrm{S} \cdot \mathrm{Min} \cdot \mathcal{F} = \forall \cdot \mathrm{S}\mathcal{F}$ *and* $\mathrm{F} \cdot \forall \cdot \mathcal{K} = \mathrm{Min} \cdot \mathrm{F}\mathcal{K}$.

Beweis.

1. Sei $A \in \mathrm{S} \cdot \mathrm{Max}\,\mathcal{F}$. Dann existieren $h \in \mathrm{Max}\,\mathcal{F}$, $g \in \mathrm{FP}$, so daß $x \in A \iff h(x) \geq g(x)$. Also existieren $f \in \mathcal{F}$, $g' \in \mathrm{FP}$, so daß

$$\begin{array}{rcl} x \in A & \iff & \max_{y \leq g'(x)} f(x,y) \geq g(x) \\ & \iff & (\exists y)(y \leq g'(x) \wedge f(x,y) \geq g(x)) \end{array}$$

Also ist $A \in \exists \mathrm{S}\mathcal{F}$.

Sei nun umgekehrt $A \in \exists \mathrm{S}\mathcal{F}$. Dann existieren $f \in \mathcal{F}$, $g, g' \in \mathrm{FP}$, so daß $x \in A \iff (\exists y \leq g'(x))(f(x,y) \geq g(x,y))$. Sei $g_1 \in \mathrm{FP}$ monoton steigend im zweiten Argument mit $g_1 \geq g$ und sei $g_2(x) =_{\mathrm{def}} g_1(x, g'(x))$. Definiere

$$f'(x,y) = f(x,y) + (g_2(x) - g(x,y)) \cdot c_{\{0,1,\ldots,g'(x)\}}(y).$$

Dann gilt:

$$\begin{array}{rcl} x \in A & \iff & (\exists y \leq g'(x))(f'(x,y) \geq g_2(x)) \\ & \iff & \max_{y \leq g'(x)} f'(x,y) \geq g_2(x) \end{array}$$

Also ist $A \in \mathrm{S}\,\mathrm{Max}\,\mathcal{F}$.

Sei $f \in \mathrm{Max\,F}\mathcal{K}$, $f(x) = \max_{y \le g(x)} \max\{\, z \mid g'(x) \le z \le g''(x) \wedge (x,y,z) \in A \,\}$ für $A \in \mathcal{K}$ and $g, g', g'' \in \mathrm{FP}$. Dann ist offensichtlich

$$f(x) = \max\{\, z \mid g'(x) \le z \le g''(x) \wedge (\exists y)(y \le g(x) \wedge (x,y,z) \in A) \,\}$$

Also ist $f \in \mathrm{F}\exists\mathcal{K}$.

Sei nun umgekehrt $h \in \mathrm{F}\exists\mathcal{K}$, $h(x) = \max\{\, z \mid g'(x) \le z \le g''(x) \wedge (\exists y)(y \le g(x) \wedge (x,y,z) \in A) \,\}$ für $A \in \mathcal{K}$, $g, g', g'' \in \mathrm{FP}$. Dann ist $h(x)$ der maximale Wert der Funktion

$$f(x,y,z) = \begin{cases} z, & \text{falls } (x,y,z) \in A \\ g'(x), & \text{sonst} \end{cases}$$

im Bereich $y \le g(x)$, $g'(x) \le z \le g''(x)$. Dann ist aber $f \in \mathrm{F}\mathcal{K}$, denn es gilt:

$$\begin{aligned} f(x,y,z) &= \max\{\, u \mid g'(x) \le u \le z \wedge (x,y,z) \in A \,\} \\ &= \max\{\, u \mid g'(x) \le u \le z \wedge (x,y,z,u) \in A' \,\} \end{aligned}$$

für geeignetes $A' \in \mathcal{K}$.

2. Aus 5.2 und 5.18 folgt:

$$\begin{aligned} \mathrm{S\,Min}\,\mathcal{F} &= \mathrm{S}(-\,\mathrm{Max}(-\mathcal{F})) = \text{co-}\mathrm{S\,Max}(-\mathcal{F}) = \text{co-}\exists\mathrm{S}(-\mathcal{F}) \\ &= \forall\text{co-co-}\mathrm{S}\mathcal{F} = \forall\mathrm{S}\mathcal{F} \end{aligned}$$

sowie

$$\begin{aligned} \mathrm{F}\forall\mathcal{K} &= \mathrm{Fco}\text{-}\exists\text{co-}\mathcal{K} = -\mathrm{F}\exists\text{co-}\mathcal{K} = -\,\mathrm{Max\,Fco}\text{-}\mathcal{K} \\ &= \mathrm{Min}(-(-\mathrm{F}\mathcal{K})) = \mathrm{Min\,F}\mathcal{K} \end{aligned}$$

□

Für den Operator Med läßt sich nur ein schwächeres Ergebnis angeben, was aber ausreichend ist, um im folgenden Abschnitt interessante Folgerungen angeben zu können.

5.28 Satz. *Sei $\mathcal{F}$ eine Funktionenklasse, für die $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$, $\mathcal{F} \cdot \mathrm{FP}_+ \subseteq \mathcal{F}$ und $\mathcal{F} + \mathrm{FP}_+ \subseteq \mathcal{F}$ gelten und sei $\mathcal{K}$ eine Mengenklasse, die unter $\le_m^{\mathrm{P}}$ abgeschlossen ist und die Klasse* P *umfaßt. Dann gilt:*

$$\mathrm{S} \cdot \mathrm{Med} \cdot \mathcal{F} = \mathrm{C} \cdot \mathrm{S}\mathcal{F} \text{ and } \mathrm{Med} \cdot \mathrm{F}\mathcal{K} \subseteq \mathrm{F} \cdot \mathrm{C} \cdot \mathcal{K} = \mathrm{FS} \cdot \mathrm{Med\,F} \cdot \mathcal{K}$$

Beweis. Sei $A \in \mathrm{S\,Med}\,\mathcal{F}$. Dann existieren $h \in \mathrm{Med}\,\mathcal{F}$, $g \in \mathrm{FP}$, so daß $x \in A \iff h(x) \ge g(x)$. Also existieren $g' \in \mathrm{FP}$ und $f \in \mathcal{F}$, so daß

$x \in A \iff \mathrm{med}_{y \le g'(x)} f(x,y) \ge g(x)$. Daraus folgt jedoch (im l-Med-Fall, analoges gilt für r-Med):

$$x \in A \iff |\{\, y \le g'(x) \mid f(x,y) \ge g(x) \,\}| \ge \frac{g'(x)}{2}$$

Also ist $A \in \mathrm{CS}\mathcal{F}$.

Sei nun umgekehrt $A \in \mathrm{CS}\mathcal{F}$. Dann existieren $f \in \mathcal{F}$, $g, g_1, f_2 \in \mathrm{FP}$, so daß $x \in A \iff |\{\, y \le g_2(x) \mid f(x,y) \ge g(x,y) \,\}| \ge g_1(x)$. Aus den Voraussetzungen an $\mathcal{F}$ ergibt sich die Existenz einer Funktion $f' \in \mathcal{F}$ und einer Funktion $g_3 \in \mathrm{FP}$ mit der Eigenschaft $x \in A \iff |\{\, y \le g_3(x) \mid f'(x,y) \ge g(x,y) \,\}| \ge \frac{g_3(x)}{2}$. Wie im Beweis von 5.2 ergeben sich die Existenz von $f'' \in \mathcal{F}$ und $g_4 \in \mathrm{FP}$, so daß

$$x \in A \iff |\{\, y \le g_3(x) \mid f''(x,y) \ge g_4(x) \,\}| \ge \frac{g_3(x)}{2}$$

Daraus folgt:

$$x \in A \iff \operatorname*{med}_{y \le g_3(x)} f''(x,y) \ge g_4(x)$$

Also ist $A \in \mathrm{S\,Med}\,\mathcal{F}$.

Da $\mathcal{K}$ unter $\le_m^{\mathrm{p}}$ abgeschlossen ist, umfaßt $\mathrm{F}\mathcal{K}$ die Klassen $\mathrm{F}\mathcal{K} \circ \mathrm{FP}$, $\mathrm{F}\mathcal{K} + \mathrm{FP}_+$ und $\mathrm{F}\mathcal{K} \cdot \mathrm{FP}_+$. Damit ergibt sich aus 5.12 und der ersten Aussage dieses Satzes $\mathrm{Med\,F}\mathcal{K} \subseteq \mathrm{FS} \cdot \mathrm{Med\,F}\mathcal{K} = \mathrm{F} \cdot \mathrm{C} \cdot \mathrm{SF}\mathcal{K} = \mathrm{FC}\mathcal{K}$. □

Wir bekommen also leider keine Gleichheit von $\mathrm{F} \cdot \mathrm{C}\mathcal{K}$ und $\mathrm{Med\,F}\mathcal{K}$. Aber wir können immerhin zeigen, daß die Differenzenklassen $\mathrm{F} \cdot \mathrm{C}\mathcal{K} - \mathrm{F} \cdot \mathrm{C}\mathcal{K}$ und $\mathrm{Med\,F}\mathcal{K} - \mathrm{Med\,F}\mathcal{K}$ unter recht allgemeinen Voraussetzungen zusammenfallen. Dazu beweisen wir zunächst ein etwas allgemeineres Resultat:

5.29 Satz. *Ist $\mathcal{F}$ eine PFO, so gilt:*

$$\mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F} - \mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F} = \mathrm{Med} \cdot \mathrm{FS}\mathcal{F} - \mathrm{Med} \cdot \mathrm{FS}\mathcal{F}.$$

Beweis. Wir beweisen als erstes, daß $\mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F} \subseteq \mathrm{Med} \cdot \mathrm{FS}\mathcal{F} - \mathrm{Med} \cdot \mathrm{FS}\mathcal{F}$ für alle PFOs $\mathcal{F}$.

Sei dazu $h \in \mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F}$,

$$h(x) = \max\{\, z \mid g_1(x) \le z < g_2(x) \wedge \operatorname*{med}_{y < g_3(x)} f(x,y,z) \ge g(x,z) \,\}$$

für $f \in \mathcal{F}$, $g, g_1, g_2 \in \mathrm{FP}$, wobei $\mathrm{med}_{y<g_3(x)} f(x,y,z+1) \ge g(x,z+1)$ impliziert, daß $\mathrm{med}_{y \le g_3(x)} f(x,y,z) \ge g(x,z)$. g_3 ist oBdA eine einstellige Funktion aufgrund von Lemma 5.5. Wir nehmen der Einfachheit halber weiterhin oBdA an,

daß g_3 nur ungerade Werte annimmt. (Dann brauchen wir die Unterscheidung r-Med/l-Med nicht zu berücksichtigen.)

Wähle $g_0 \in$ FP so, daß $f(x,y,z) \in [g_0(x)]$ für z mit $g_1(x) \leq z \leq g_2(x)$ sowie y mit $0 \leq y < g_3(x)$. Wähle $g' \in$ FP so, daß $g_0(x) \cdot g_3(x) \leq g'(x)$ und $g_1(x) \leq z \leq g_2(x)$ impliziert, daß $z \in [g'(x)]$. OBdA nehmen wir an, daß $g_2(x) - g_1(x)$ eine Zweierpotenz ist und setzen $p(x) =_{\text{def}} \log(g_2(x) - g_1(x))$. Wir schreiben im Verlauf des weiteren Beweises auch abkürzend p statt $p(x)$.

Da $\mathcal{F}$ eine PFO ist, existieren $\hat{f} \in \mathcal{F}$, $\hat{g} \in$ FP und r, so daß für z_i mit $g_1(x) \leq z_i \leq g_2(x)$ und für y_i mit $0 \leq y_i < g_3(x)$ $(1 \leq i \leq p(x))$ gilt:

$$\begin{aligned}
&\hat{f}(x, \langle y_{p(x)}, z_{p(x)}, \ldots, y_1, z_1\rangle_{g'(x)}) \\
&\quad = \langle r(x, y_{p(x)}, z_{(p(x)}), y_{p(x)} + g_3(x) \cdot f(x, y_{p(x)}, z_{p(x)}), \ldots \\
&\qquad\qquad r(x, y_1, z_1), y_1 + g_3(x) \cdot f(x, y_1, z_1)\rangle_{\hat{g}(x), g'(x)}.
\end{aligned}$$

Definiere induktiv Zahlen $(z(1), \ldots, z(p(x)+1)) =_{\text{def}} Z(c_1, \ldots, c_{p(x)})$ wie folgt:

$$\begin{aligned}
z(1) &= \tfrac{g_1(x)+g_2(x)}{2} \\
z(i+1) &= \begin{cases} z(i) + \frac{g_2(x)-g_1(x)}{2^{i+1}}, & \text{falls } c_i \geq g(x, z(i)) \\ z(i) - \frac{g_2(x)-g_1(x)}{2^{i+1}}, & \text{falls } c_i < g(x, z(i)) \end{cases}, i = 1 \ldots p(x) - 1 \\
z(i+1) &= \begin{cases} z(i), & \text{falls } c_i \geq g(x, z(i)) \\ z(i) - 1, & \text{falls } c_i < g(x, z(i)) \end{cases}, i = p(x)
\end{aligned}$$

Definiere weiterhin eine Menge A_1, so daß für $y_1, \ldots, y_p$ mit $0 \leq y_1, \ldots, y_p < g_3(x)$ und für $c_1, \ldots, c_p \in [g_0(x)]$ gilt:

$$(x, \langle y_1, \ldots, y_p\rangle_{g'(x)}, d) \in A_1 \iff \langle u', \hat{f}(x, \langle y_p, z(p), \ldots, y_1, z(1)\rangle_{g'(x)})\rangle_{g'(x)} \geq d,$$

wobei $d = \langle u, \langle r_p, y_p + g_3(x)c_p, \ldots, r_1, y_1 + g_3(x)c_1\rangle_{\hat{g}(x), g'(x)}\rangle_{g'(x)}$ und $u' = z(p+1)$ wie oben definiert. Dann ist $A_1 \in \mathrm{S}\mathcal{F}$. Definiere A_2 analog zu A_1 mit dem einzigen Unterschied, daß wir nun für u' fordern, daß $u' = 0$.

Definiere für $i = 1, 2$

$$f_i(x, \langle y_1, \ldots, y_p\rangle) =_{\text{def}} \max\{\, d \text{ in geeignetem Bereich} \mid (x, \langle y_1, \ldots, y_p\rangle, d) \in A_i \,\}$$

Dann gilt:

$$\begin{aligned}
&f_1(x, \langle y_1, \ldots, y_p\rangle) = \\
&\qquad \langle z_{p+1}, \langle r(x, y_p, z_p), \langle y_p, f(x, y_p, z_p)\rangle, \ldots, r(x, y_1, z_1), \langle y_1, f(x, y_1, z_1)\rangle\rangle\rangle \\
&f_2(x, \langle y_1, \ldots, y_p\rangle) = \\
&\qquad \langle \quad 0, \langle r(x, y_p, z_p), \langle y_p, f(x, y_p, z_p)\rangle, \ldots, r(x, y_1, z_1), \langle y_1, f(x, y_1, z_1)\rangle\rangle\rangle
\end{aligned}$$

wobei $\langle z_1, \ldots, z_p\rangle = Z(f(x, y_1, z_1), \ldots, f(x, y_p, z_p))$.

Die Funktion f_1 simuliert jedoch die Berechnung von $h(x)$ mittels binärer Suche nach dem maximalen Wert z wie in der Definition von h angegeben. Betrachten wir den mittleren Wert aller $f_1(x, \langle y_1, \ldots, y_p \rangle_{g'(x)})$ über alle $\langle y_1, \ldots, y_p \rangle_{g'(x)}$. Für ihn gilt sicherlich, daß $f(x, y_1, z(1)) \geq g(x, z(1))$ genau dann, wenn $h(x) \geq z(1)$. Die nächste Annäherung $z(2)$ im Verlauf der binären Suche ist nun $z(1)$ erhöht oder vermindert um eine geeignete Zweierpotenz. Erneut ist gilt für den Median, daß $f(x, y_2, z(2)) \geq g(x, z(2))$ genau dann, wenn $h(x) \geq z(2)$, usw. Die Folge $z(1), z(2), \ldots$ konvergiert also gegen $z(p+1) = h(x)$. Die erste Komponente des mittleren Wertes aller $f_1(x, \langle y_1, \ldots, y_p \rangle_{g'(x)})$ über $\langle y_1, \ldots, y_p \rangle_{g'(x)}$ ist also genau der Wert von $h(x)$. Subtrahieren wir nun den mittleren Wert aller $f_2(x, \langle y_1, \ldots, y_p \rangle_{g'(x)})$ von dem mittleren Wert aller $f_1(x, \langle y_1, \ldots, y_p \rangle_{g'(x)})$, erhalten wir $h(x)$. Also ist $\mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F} \subseteq \mathrm{Med} \cdot \mathrm{FS}\mathcal{F} - \mathrm{Med} \cdot \mathrm{FS}\mathcal{F}$.

Kommen wir nun zurück zur Aussage des Satzes:

($\supseteq$): Mit 5.28 und 5.15 ergibt sich: $\mathrm{Med} \cdot \mathrm{FS}\mathcal{F} - \mathrm{Med} \cdot \mathrm{FS}\mathcal{F} \subseteq \mathrm{F} \cdot \mathrm{C} \cdot \mathrm{S}\mathcal{F} - \mathrm{F} \cdot \mathrm{C} \cdot \mathrm{S}\mathcal{F} \subseteq \mathrm{FP}^{\mathrm{C} \cdot \mathrm{S}\mathcal{F}} \subseteq \mathrm{FP}^{\mathrm{Med}\,\mathcal{F}} \subseteq \mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F} - \mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F}$.

($\subseteq$): Wir nehmen zunächst vereinfachend an, daß $h(x) = h_1(x) + h_2(x)$, $h_i(x) = \mathrm{med}_{y < g(x)} f_i(x, y)$, $f_i \in \mathrm{FS}\mathcal{F}$, $g \in \mathrm{FP}$ für $i \in \{1, 2\}$. (Wir nehmen wegen Lemma 5.5 oBdA nur eine Bereichsfunktion g an.) Da $\mathrm{FS}\mathcal{F}$ eine PFO ist, existieren $\hat{f} \in \mathrm{FS}\mathcal{F}$ und r, so daß

$$\hat{f}(x, y_1, y_2) = \langle r(x, y_2), y_2 + g(x) f_2(x, y_2), r(x, y_1), y_1 + g(x) f_1(x, y_1) \rangle$$

Da $f_1 + f_2 \in \mathrm{FP}^{\mathcal{F}}$, existieren $f_1^*, f_2^* \in \mathrm{FS}\mathcal{F}$ mit $f_1 + f_2 = f_1^* - f_2^*$ (wegen Satz 5.15). Definiere

$$\begin{aligned} f(x, \langle y_1, y_2 \rangle) &= \langle f_1^*(x, y_1), \hat{f}(x, y_1, y_2) \rangle \\ f'(x, \langle y_1, y_2 \rangle) &= \langle f_2^*(x, y_2), \hat{f}(x, y_1, y_2) \rangle \end{aligned}$$

Ist $\mathcal{F}$ eine PFO, so folgt $f, f' \in \mathrm{FS}\mathcal{F}$.

Da jedoch

$$h(x) = \operatorname*{med}_{\substack{y_1 \leq g_1(x) \\ y_2 \leq g_2(x)}} f(x, \langle y_1, y_2 \rangle) - \operatorname*{med}_{\substack{y_1 \leq g_1(x) \\ y_2 \leq g_2(x)}} f'(x, \langle y_1, y_2 \rangle)$$

ergibt sich $h \in \mathrm{Med}\,\mathrm{FS}\mathcal{F} - \mathrm{Med}\,\mathrm{FS}\mathcal{F}$.

Diese Argumentation kann nun leicht dahingehend erweitert werden, daß eine höhere Anzahl von Funktionen arithmetisch verknüpft wird. Daraus ergibt sich: $(\mathrm{Med}\,\mathrm{FS}\mathcal{F} - \mathrm{Med}\,\mathrm{FS}\mathcal{F}) - (\mathrm{Med}\,\mathrm{FS}\mathcal{F} - \mathrm{Med}\,\mathrm{FS}\mathcal{F}) \subseteq \mathrm{Med}\,\mathrm{FS}\mathcal{F} - \mathrm{Med}\,\mathrm{FS}\mathcal{F}$. Aus $\mathrm{FS} \cdot \mathrm{Med}\,\mathcal{F} \subseteq \mathrm{Med} \cdot \mathrm{FS}\mathcal{F} - \mathrm{Med} \cdot \mathrm{FS}\mathcal{F}$ wie oben gezeigt, folgt nun die Aussage des Satzes. $\square$

Die oben angesprochene Gleichheit der Differenzenklassen folgt nun leicht:

5.30 Korollar. *Ist $\mathcal{K}$ eine APK, so gilt:*

$$\mathrm{FC}\mathcal{K} - \mathrm{FC}\mathcal{K} = \mathrm{Med}\,\mathrm{F}\mathcal{K} - \mathrm{Med}\,\mathrm{F}\mathcal{K}.$$

Beweis. $\mathrm{FC}\mathcal{K} = \mathrm{FS}\cdot\mathrm{Med}\,\mathrm{F}\mathcal{K}$ aufgrund von 5.28. $\mathrm{Med}\,\mathrm{F}\mathcal{K} = \mathrm{Med}\,\mathrm{FS}\cdot\mathrm{F}\mathcal{K}$ aufgrund von 5.12. Wir wenden nun 5.29 auf die PFO $\mathcal{F} = \mathrm{F}\mathcal{K}$ an.

□

5.5.2. Fixpunkte des Operators FS

Wir wenden uns nun der Identifizierung von Fixpunkten von FS unter den angesprochenen Funktionenklassen zu. Dazu zunächst ein Hilfssatz:

5.31 Satz. *Ist $\mathcal{F}$ eine PFO, so gilt:*

$$\mathrm{FS}\cdot\mathcal{F} \subseteq \mathrm{Max}\,\mathcal{F} - \mathrm{FP}$$

Beweis. Sei $h \in \mathrm{FS}\mathcal{F}$, $h(x) = \max\{\, y \mid g_1(x) \le y < g_2(x) \wedge f_1(x,y) \ge g(x,y)\,\}$ für $f_1 \in \mathcal{F}$ und $g, g_1, g_2 \in \mathrm{FP}$, so daß $f_1(x, y+1) \ge g(x, y+1) \Rightarrow f_1(x,y) \ge g(x,y)$. Wie im Beweis von 5.2 ergibt sich die Existenz von $f_2 \in \mathcal{F}$, $g_3 \in \mathrm{FP}$ so daß $h(x) = \max\{\, y \mid g_1(x) \le y < g_2(x) \wedge f_2(x,y) \ge g_3(x)\,\}$ wobei $f_2(x, y+1) \ge g_3(x) \Rightarrow f_2(x,y) \ge g_3(x)$. Definiere

$$f_3(x,y) = \max\{g_3(x) - 1, \min\{f_2(x,y), g_3(x)\}\}$$

Es gilt: $f_3 \in \mathcal{F}$, $f_3(x,y) \in \{g_3(x)-1, g_3(x)\}$, und $f_3(x, y+1) \ge g_3(x) \Rightarrow f_3(x,y) \ge g_3(x)$. Außerdem gilt:

$$h(x) = \max\{\, y \mid g_1(x) \le y < g_2(x) \wedge f_3(x,y) = g_3(x)\,\}.$$

Wähle $g_4 \in \mathrm{FP}$, $g_4 > 0$, mit $g_1(x) \le y < g_2(x) \Rightarrow y \in [g_4(x) - 1]$. Dann ergibt sich folgendes (wir lassen aus Gründen der Übersichtlichkeit die Schranken $g_1(x) \le y \le g_2(x)$ weg):

$$\begin{aligned} h(x) &= \max\{\, y \mid f_3(x,y)\cdot 2g_4(x) + g_4(x) = g_3(x)\cdot 2g_4(x) + g_4(x)\,\} \\ &= \max\{\, y \mid f_3(x,y)\cdot 2g_4(x) + g_4(x) + y \ge g_3(x)\cdot 2g_4(x) + g_4(x)\,\} \\ &= \max\nolimits_y (f_3(x,y)\cdot 2g_4(x) + g_4(x) + y) - g_3(x)\cdot 2g_4(x) - g_4(x) \end{aligned}$$

□

Nun können wir zeigen, daß für allgemeine PFOs $\mathcal{F}$ die Klassen $\mathrm{Max}\,\mathcal{F} - \mathrm{FP}$ und $\mathrm{Min}\,\mathcal{F} - \mathrm{FP}$ Fixpunkte von FS sind.

5.32 Korollar. *Sei $\mathcal{F}$ eine PFO. Dann gilt:*

1. $\mathrm{FS}(\mathrm{Max}\,\mathcal{F} - \mathrm{FP}) = \mathrm{FS} \cdot \mathrm{Max}\,\mathcal{F} = \mathrm{Max} \cdot \mathrm{FS}\mathcal{F} = \mathrm{Max}\,\mathcal{F} - \mathrm{FP}$.
2. $\mathrm{FS}(\mathrm{Min}\,\mathcal{F} - \mathrm{FP}) = \mathrm{FS} \cdot \mathrm{Min}\,\mathcal{F} = \mathrm{Min} \cdot \mathrm{FS}\mathcal{F} = \mathrm{Min}\,\mathcal{F} - \mathrm{FP}$.

Beweis. Aus 5.12 folgt $\mathrm{FS}(\mathrm{Max}\,\mathcal{F} - \mathrm{FP}) = \mathrm{FS}\,\mathrm{Max}\,\mathcal{F}$ und $\mathrm{FS}(\mathrm{Min}\,\mathcal{F} - \mathrm{FP}) = \mathrm{FS}\,\mathrm{Min}\,\mathcal{F}$. Aus 5.31 und 5.3 folgt: $\mathrm{FS}\,\mathrm{Max}\,\mathcal{F} \subseteq \mathrm{Max}\,\mathrm{Max}\,\mathcal{F} - \mathrm{FP} \subseteq \mathrm{Max}\,\mathcal{F} - \mathrm{FP}$. Aus 5.12 folgt: $\mathrm{Max}\,\mathcal{F} - \mathrm{FP} \subseteq \mathrm{FS}(\mathrm{Max}\,\mathcal{F} - \mathrm{FP})$. Für Min ergibt sich aufgrund von 5.18 und 5.3: $\mathrm{FS}\,\mathrm{Min}\,\mathcal{F} = -\mathrm{FS}\,\mathrm{Max}(-\mathcal{F}) = -(\mathrm{Max}(-\mathcal{F}) - \mathrm{FP}) = -\mathrm{Max}(-\mathcal{F}) - \mathrm{FP} = \mathrm{Min}\,\mathcal{F} - \mathrm{FP}$ Aus 5.12 folgt $\mathrm{Min}\,\mathcal{F} - \mathrm{FP} \subseteq \mathrm{FS}(\mathrm{Min}\,\mathcal{F} - \mathrm{FP})$. □

Aus 5.32 und 5.15 folgt nun direkt:

5.33 Korollar. *Sei $\mathcal{F}$ eine PFO. Dann gilt:*

1. $\mathrm{FP}^{\mathrm{Max}\,\mathcal{F}} = \mathrm{Max}\,\mathcal{F} - \mathrm{Max}\,\mathcal{F}$.
2. $\mathrm{FP}^{\mathrm{Min}\,\mathcal{F}} = \mathrm{Min}\,\mathcal{F} - \mathrm{Min}\,\mathcal{F}$.

Da wir $\mathrm{FS}\,\mathrm{Med}\,\mathcal{F} = \mathrm{Med}\,\mathcal{F} - \mathrm{FP}$ nicht allgemein für alle PFOs $\mathcal{F}$ zeigen konnten, können wir nun auch kein Resultat analog zu Korollar 5.33 für Medianklassen angeben. Aus Satz 5.15 folgt lediglich $\mathrm{FP}^{\mathrm{Med}\,\mathcal{F}} = \mathrm{FS}\,\mathrm{Med}\,\mathcal{F} - \mathrm{FS}\,\mathrm{Med}\,\mathcal{F}$. Aus Satz 5.29 ergibt sich, daß diese Klasse gleich $\mathrm{Med} \cdot \mathrm{FS}\mathcal{F} - \mathrm{Med} \cdot \mathrm{FS}\mathcal{F}$ ist.

5.5.3. Hierarchien

Wir definieren nun eine Funktionenhierarchie in Analogie zur Polynomialzeit-Hierarchie von Mengen.

5.34 Definition. Sei $\mathcal{F}$ eine Funktionenklasse. Die Klassen der *Min-Max-Hierarchie über $\mathcal{F}$* sind dann

$$\begin{aligned} \Sigma_0^p\mathcal{F} &= \Pi_0^p\mathcal{F} = \Delta_0^p\mathcal{F} = \mathcal{F} \\ \Sigma_{k+1}^p\mathcal{F} &= \mathrm{Max}\,\Pi_k^p\mathcal{F} \\ \Pi_{k+1}^p\mathcal{F} &= \mathrm{Min}\,\Sigma_k^p\mathcal{F} \\ \Delta_{k+1}^p\mathcal{F} &= \mathrm{FP}^{\Sigma_k^p\mathcal{F} \cup \Pi_k^p\mathcal{F}} \end{aligned}$$

Weiterhin setzen wir

$$\mathrm{FPH} \cdot \mathcal{F} = \bigcup_{k \geq 0} \Delta_k^p\mathcal{F}.$$

Offensichtliche induktive Verallgemeinerungen der Lemmata 5.2 und 5.3 ergeben folgende einfache Eigenschaften dieser Klassen:

5.35 Lemma. *Sei $\mathcal{F}$ eine PFO. Dann gilt:*

1. $\Sigma_k^p(\mathcal{F} - \mathrm{FP}) = \Sigma_k^p\mathcal{F} - \mathrm{FP}$.
2. $\Pi_k^p(\mathcal{F} - \mathrm{FP}) = \Pi_k^p\mathcal{F} - \mathrm{FP}$.
3. $\Sigma_k^p(-\mathcal{F}) = -\Pi_k^p\mathcal{F}$ *und* $\Sigma_k^p(\mathrm{FP} - \mathcal{F}) = \mathrm{FP} - \Pi_k^p\mathcal{F}$.
4. $\Pi_k^p(-\mathcal{F}) = -\Sigma_k^p\mathcal{F}$ *und* $\Pi_k^p(\mathrm{FP} - \mathcal{F}) = \mathrm{FP} - \Sigma_k^p\mathcal{F}$.

Eine ebenso einfache induktive Verallgemeinerung von Satz 5.27 zeigt, daß unter den Konversionsoperatoren S und F die Klassen der Min-Max-Hierarchie über einer Funktionenklasse $\mathcal{F}$ bzw. $\mathrm{F}\cdot\mathcal{K}$ und die Klassen der Polynomialzeithierarchie über der Mengenklasse $\mathrm{S}\cdot\mathcal{F}$ bzw. $\mathcal{K}$ einander entsprechen.

5.36 Satz. *Sei $\mathcal{F}$ eine PFO und $\mathcal{K}$ eine APK. Dann gilt für alle $k \geq 1$:*

1. $\mathrm{S}\cdot\Sigma_k^p\mathcal{F} = \Sigma_k^p(\mathrm{S}\mathcal{F})$ *und* $\mathrm{F}\cdot\Sigma_k^p\mathcal{K} = \Sigma_k^p(\mathrm{F}\mathcal{K})$.
2. $\mathrm{S}\cdot\Pi_k^p\mathcal{F} = \Pi_k^p(\mathrm{S}\mathcal{F})$ *und* $\mathrm{F}\cdot\Pi_k^p\mathcal{K} = \Pi_k^p(\mathrm{F}\mathcal{K})$.

Dies bedeutet jedoch noch nicht, daß die $\Sigma_k^p\mathcal{F}$'s und $\Pi_k^p\mathcal{F}$'s allgemein Fixpunkte von FS sind. Aus Satz 5.32 folgt aber unmittelbar:

5.37 Korollar. *Sei $\mathcal{F}$ eine PFO. Dann gilt für alle $k \geq 1$:*

1. $\mathrm{FS}(\Sigma_k^p\mathcal{F} - \mathrm{FP}) = \mathrm{FS}\cdot\Sigma_k^p\mathcal{F} = \Sigma_k^p(\mathrm{FS}\mathcal{F}) = \Sigma_k^p\mathcal{F} - FP$.
2. $\mathrm{FS}(\Pi_k^p\mathcal{F} - \mathrm{FP}) = \mathrm{FS}\cdot\Pi_k^p\mathcal{F} = \Pi_k^p(\mathrm{FS}\mathcal{F}) = \Pi_k^p\mathcal{F} - \mathrm{FP}$.

Zusammen mit Satz 5.15 folgt daraus direkt:

5.38 Korollar. *Sei $\mathcal{F}$ eine PFO. Dann gilt für alle $k \geq 1$:*

1. $\mathrm{FP}^{\Sigma_k^p\mathcal{F}} = \Sigma_k^p\mathcal{F} - \Sigma_k^p\mathcal{F} = \Sigma_k^p\mathcal{F} + \Pi_k^p(-\mathcal{F})$.
2. $\mathrm{FP}^{\Pi_k^p\mathcal{F}} = \Pi_k^p\mathcal{F} - \Pi_k^p\mathcal{F} = \Pi_k^p\mathcal{F} + \Sigma_k^p(-\mathcal{F})$.

Wir wenden uns nun der Frage des Enthaltenseins der Δ-Stufen der Min-Max-Hierarchie in den nächsten Σ- und Π-Stufen zu. Für allgemeine PFOs können wir ein Resultat dieser Form nicht erwarten, da sicherlich im allgemeinen Max oder Min keine Subtraktion „simulieren“ können. Unter einer zusätzlichen Voraussetzung ist dies jedoch möglich.

5.39 Lemma. *Sei $\mathcal{F}$ eine PFO. Dann gilt:*

1. $\mathrm{FP}^{\mathcal{F}} \subseteq \mathrm{Min}\max(\mathcal{F} - \mathrm{FP}, \mathrm{FP} - \mathcal{F})$.

2. $\mathrm{FP}^{\mathcal{F}} \subseteq \mathrm{Max}\min(\mathcal{F} - \mathrm{FP}, \mathrm{FP} - \mathcal{F})$.

Beweis. Werde f von der deterministischen Polynomialzeit-Maschine M mit Orakel $h \in \mathcal{F}$ berechnet. OBdA nehmen wir an, daß M bei Eingabe x genau $p(|x|)$ Fragen (für ein $p \in \mathrm{Pol}$) an h stellt. Weiterhin nehmen wir an, daß bei Eingabe x nur Fragen z gestellt werden, für die $h(z) \in [g(x)]$ für eine geeignete Funktion $g \in \mathrm{FP}$ gilt. Da $\mathcal{F}$ unter Tupelbildung abgeschlossen ist, können wir die $p(|x|)$ Fragen an h mit einer einzigen Frage an eine andere Funktion $h' \in \mathcal{F}$ simulieren. h' antwortet mit Sequenzen der Form

$$y = \langle y'_{p(|x|)}, y_{p(|x|)} \ldots, y'_2, y_2, y'_1, y_1 \rangle$$

wobei $y_i \in [g(x)]$ und $y'_i \in [\hat{g}(x)]$ für $i = 1, 2, \ldots, p(|x|)$ und eine Funktion $\hat{g} \in \mathrm{FP}$. Im folgenden bezeichne y stets Zahlen dieser Form.

Sei $r_M(x, y, k)$ die k-th Frage von M bei Eingabe x, falls $y_1, y_2, \ldots, y_{k-1}$ die Antworten von h auf die vorherigen $k-1$ Fragen sind. Sei $g_M(x, y)$ die Ausgabe von M bei Eingabe x, falls y von der obigen Form ist und $y_1, y_2, \ldots, y_{p(|x|)}$ die Antworten von h in dieser Rechnung sind. Sei $g' \in \mathrm{FP}_+$, so daß $g_M(x, y) \in [g'(x) - 1]$ für alle y von der obigen Form.

Offenbar ist y genau dann die Antwort von h' auf die Folge der korrekten Orakelfragen der Rechnung von M auf Eingabe x, wenn gilt:

$$y = \hat{h}(x, y) =_{\mathrm{def}} h'(x, \langle r_M(x, y, 1), r_M(x, y, 2), \ldots, r_M(x, y, p(|x|)) \rangle).$$

Da $h' \in \mathcal{F}$, ist auch $\hat{h} \in \mathcal{F}$. Das y mit $y = \hat{h}(x, y)$ kodiert also die korrekten Orakelantworten, aber auch bestimmte „Einschübe", die sich durch die Tupelfunktion ergeben.

Ist nun y_x solch ein korrektes y (d. h. $y_x = \hat{h}(x, y_z)$), so gilt:

$$\begin{aligned} f(x) &= g_M(x, y_x) \\ &= \min_{y \text{ wie oben}} \max\{(\hat{h}(x, y) - y) \cdot g'(x) + g_M(x, y), \\ &\qquad\qquad (y - \hat{h}(x, y)) \cdot g'(x) + g_M(x, y)\} \end{aligned}$$

Der minimale Term über alle y von der oben beschriebenen Form ergibt sich für $y = \hat{h}(x, y)$, also ist der minimale Term genau gleich dem Wert $f(x)$.

Der Beweis von Aussage 2 verläuft analog. □

Nun ergibt sich bezogen auf die obige Fragestellung:

5.40 Satz. *Sei $\mathcal{F}$ eine PFO und sei $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$. Dann gilt für alle $k \geq 1$:*

1. $\Delta^p_{k+1}\mathcal{F} = \mathrm{FP}^{\Sigma^p_k \mathcal{F}} = \mathrm{FP}^{\Pi^p_k \mathcal{F}} \subseteq (\Sigma^p_{k+1}\mathcal{F} - \mathrm{FP}) \cap (\Pi^p_{k+1}\mathcal{F} - \mathrm{FP})$.

2. $\mathrm{Max}\,\Delta^p_{k+1}\mathcal{F} = \Sigma^p_{k+1}\mathcal{F} - \mathrm{FP}$.

3. $\mathrm{Min}\,\Delta^p_{k+1}\mathcal{F} = \Pi^p_{k+1}\mathcal{F} - \mathrm{FP}$.

Beweis. Aus 5.35 folgt: $\mathrm{FP}^{\Sigma^p_k\mathcal{F}} \subseteq \mathrm{FP}^{\Sigma^p_k(\mathrm{FP}-\mathcal{F})} = \mathrm{FP}^{\mathrm{FP}-\Pi^p_k\mathcal{F}} = \mathrm{FP}^{\Pi^p_k\mathcal{F}}$. Die andere Richtung wird vollkommen analog bewiesen.

Außerdem folgt:

$$\begin{array}{rll}
\mathrm{FP}^{\Sigma^p_k\mathcal{F}} & \subseteq \mathrm{Max}\,\mathrm{min}(\Sigma^p_k\mathcal{F} - \mathrm{FP}, \mathrm{FP} - \Sigma^p_k\mathcal{F}) & \text{wegen } 5.39 \\
& \subseteq \mathrm{Max}\,\mathrm{min}(\Sigma^p_k\mathcal{F} - \mathrm{FP}, \Pi^p_k\mathcal{F} - \mathrm{FP}) & \text{wegen } 5.35 \\
& \subseteq \mathrm{Max}\,\mathrm{min}(\Sigma^p_{k+1}\mathcal{F} - \mathrm{FP}, \Sigma^p_{k+1}\mathcal{F} - \mathrm{FP}) & \text{wegen } 5.6 \\
& \subseteq \mathrm{Max}\,\mathrm{min}(\Pi^p_k\mathcal{F} - \mathrm{FP}, \Pi^p_k\mathcal{F} - \mathrm{FP}) & \text{wegen } 5.3, 3. \\
& \subseteq \mathrm{Max}\,\mathrm{Min}\,\Pi^p_k\mathcal{F} - \mathrm{FP} & \text{wegen } 5.3, 2. \\
& \subseteq \Sigma^p_{k+1}\mathcal{F} - \mathrm{FP} & \text{wegen } 5.3, 2.
\end{array}$$

Die Aussagen 2 und 3 folgen direkt aus Aussage 1. □

Unter den Voraussetzungen des vorherigen Satzes ergeben sich nun folgende interessante Resultate: Zum einen kann jede Funktion aus einer Δ-Stufe einer Min-Max-Hierarchie geschrieben werden als Differenz zweier Funktionen aus den vorherigen Σ- oder Π-Stufen. Außerdem ergibt sich, daß die Vereinigung aller Klassen der Hierarchie gleich dem Abschluß der Basisklasse unter Min und Max oder unter Max und Subtraktion oder unter Min und Subtraktion ist.

5.41 Korollar. *Sei $\mathcal{F}$ eine PFO und sei $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$. Dann gilt für alle $k \geq 1$:*

1. $\Delta^p_{k+1}\mathcal{F} = \Sigma^p_k\mathcal{F} - \Sigma^p_k\mathcal{F} = \Pi^p_k\mathcal{F} - \Pi^p_k\mathcal{F} = \mathrm{FP}^{\Sigma^p_k\mathcal{F}}[1] = \mathrm{FP}^{\Pi^p_k\mathcal{F}}[1]$.

2. $\mathrm{FPH}\cdot\mathcal{F} = \Gamma_{\mathrm{Max,Min}}(\mathcal{F}) - \mathrm{FP} = \Gamma_{\mathrm{Max},-}(\mathcal{F}) = \Gamma_{\mathrm{Min},-}(\mathcal{F})$.

3. $\mathrm{FPH}\cdot\mathcal{F} = \mathrm{F}\cdot\mathrm{PH}\cdot\mathrm{S}\mathcal{F}$ *ist ein Fixpunkt von* FS.

Die Resultate dieses Abschnitts (unter den Voraussetzungen von Korollar 5.41) werden in Bild 5.2 zusammengefaßt. Alle dort angegebenen Funktionenklassen sind Fixpunkte von FS. Klassen mit gleicher Position in der linken oder rechten Hälfte der Abbildung werden unter F und S ineinander transformiert. Zwei Klassen in einer Hälfte sind genau dann gleich, wenn die entsprechenden Klassen der anderen Hälfte gleich sind.

Ähnlich wie oben können wir mit dem Operator Med eine Hierarchie definieren, die der Counting-Hierarchie von Mengen entspricht. Da das Med-Resultat aus Satz 5.28 schwächer ist als die entsprechenden Resultate für Max und Min

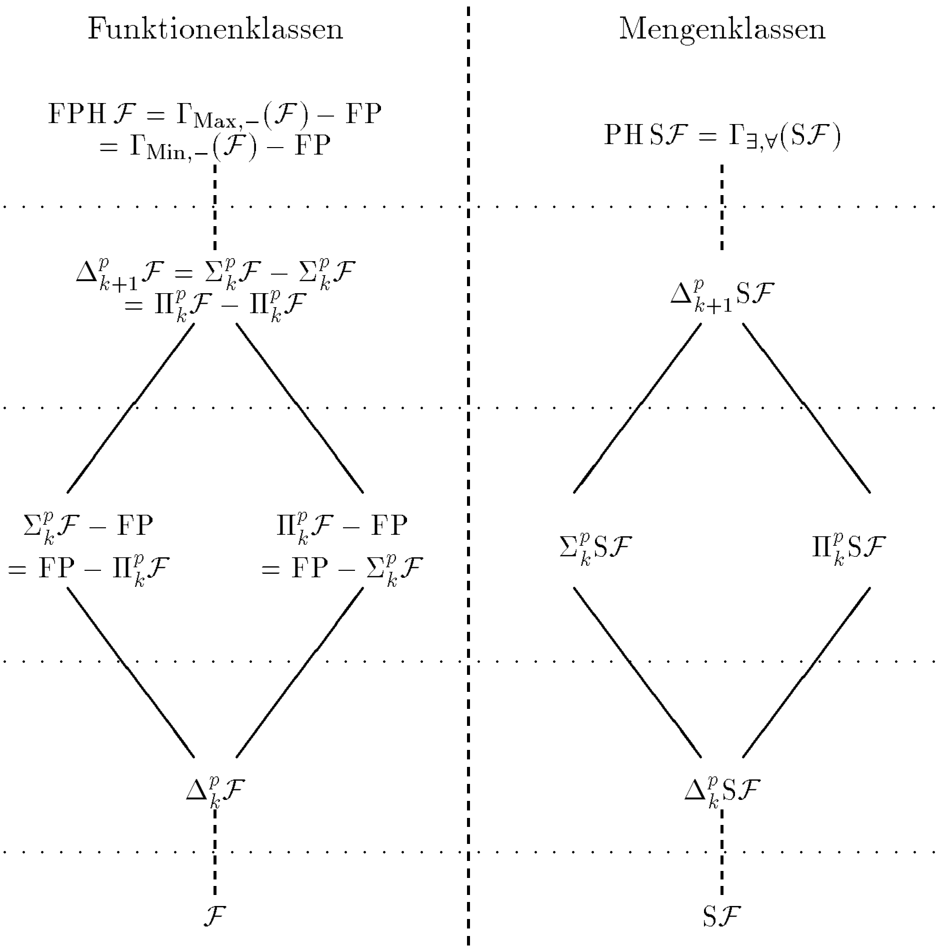

Abbildung 5.2: Die Min-Max-Hierarchie

aus 5.27, können wir nicht zeigen, daß die Klassen der Form $\mathrm{Med}^k \cdot \mathcal{F} - \mathrm{FP}$ Fixpunkte von FS sind (wie wir es analog für Max und Min in Korollar 5.37 konnten). Dennoch ergeben sich auf für die Med-Hierarchie interessante strukturelle Einsichten, die denen der Min-Max-Hierarchie sehr ähnlich sind.

Wir beginnen mit einer offensichtlichen induktiven Verallgemeinerung von Satz 5.28:

5.42 Satz. *Sei $\mathcal{F}$ eine PFO und sei $\mathcal{K}$ eine APK. Dann gilt:*

$$\mathrm{S} \cdot \mathrm{Med}^k \mathcal{F} = \mathrm{C}^k \cdot \mathrm{S}\mathcal{F} \textit{ und } \mathrm{F} \cdot \mathrm{C}^k \mathcal{K} = \mathrm{FS}\,\mathrm{Med}^k \cdot \mathrm{F}\mathcal{K}.$$

Erneut erwarten wir nicht, daß im allgemeinen Fall die Klassen $\mathrm{FP}^{\mathrm{Med}^k \mathcal{F}}$ in den nächsthöheren Stufen $\mathrm{Med}^{k+1} \mathcal{F}$ enthalten sind. Aber es zeigt sich, daß wir unter der gleichen zusätzlichen Voraussetzung wie oben im Min-Max-Fall einen derartigen Zusammenhang beweisen können:

5.43 Lemma. *Sei $\mathcal{F}$ eine PFO und sei $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$. Dann gilt:*

1. $\mathrm{FP}^{\mathcal{F}} \subseteq \mathrm{Med}\,\mathcal{F} - \mathrm{FP}$.
2. $\mathrm{Med}\,\mathrm{FP}^{\mathcal{F}} = \mathrm{Med}\,\mathcal{F} - \mathrm{FP}$.

Beweis.

1. Sei $f \in \mathrm{FP}^h$, $h \in \mathcal{F}$. Wir definieren zunächst Funktionen g', g_M und $\hat{h}$ wie im Beweis von Lemma 5.39. Dann fahren wir wie folgt fort:

$$\begin{aligned} f(x) &= g_M(x, y_x) \\ &= \underset{\substack{y \text{ wie oben} \\ b \in \{-1,+1\}}}{\mathrm{med}} \left[b \cdot (\hat{h}(x,y) - y) \cdot g'(x) + g_M(x,y) \right] \end{aligned}$$

Da $\mathcal{F}$ eine PFO ist, und da $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$, existieren Funktionen $h_1 \in \mathcal{F}, g_1 \in \mathrm{FP}_+$, so daß $\hat{h}(x,y) = g_1(x,y) - h_1(x,y)$, also folgt: $-(\hat{h}(x,y) - y) = h_1(x,y) - g_1(x,y) + y$. Definiere

$$h_2(x,y,b) =_{\mathrm{def}} \begin{cases} (\hat{h}(x,y) - y) g'(x) + g_M(x,y), & \text{falls } b \geq 1; \\ (h_1(x,y) - g_1(x,y) + y) g'(x) + g_M(x,y), & \text{falls } b \leq 0. \end{cases}$$

Dann ist $h_2 \in \mathcal{F} - \mathrm{FP}$ (Definition durch Fallunterscheidung). Es gilt jedoch:

$$f(x) = \underset{\substack{y \text{ wie oben} \\ 0 \leq b \leq 1}}{\mathrm{med}} h_2(x,y,b),$$

also ist $f \in \mathrm{Med}\,\mathcal{F} - \mathrm{FP}$.

2. Der Beweis von Aussage 1 zeigt, daß das Ergebnis der simulierten $\mathrm{FP}^{\mathcal{F}}$-Berechnung der mittlere Wert einer exponentiell langen Folge von Werten (je einer für jede mögliche Kodierung y von Orakelantworten) ist. Haben wir nun den Median einer exponentiellen Folge von $\mathrm{FP}^{\mathcal{F}}$-Berechnungen zu bestimmen, so simulieren wir jede einzelne Berechnung wie oben und verschränken die einzelnen Simulationen. Dann sind die Ausgaben der einzelnen $\mathrm{FP}^{\mathcal{F}}$-Berechnungen die Werte in der Mitte, und der mittlere Wert über alle $\mathrm{FP}^{\mathcal{F}}$-Berechnungen ist der Median der Gesamtfolge.

□

Es ergibt sich nun folgendes Resultat:

5.44 Satz. *Sei $\mathcal{F}$ eine PFO und sei $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$. Dann gilt für alle $k \geq 1$:*

1. $\mathrm{FP}^{\mathrm{Med}^k \mathcal{F}} = \mathrm{Med}^k \mathcal{F} - \mathrm{Med}^k \mathcal{F} = \mathrm{Med}^k \mathcal{F} + \mathrm{Med}^k \mathcal{F} - \mathrm{FP}$.

2. $\mathrm{FP}^{\mathrm{Med}^{k-1} \mathcal{F}} \subseteq \mathrm{Med}\,\mathrm{FP}^{\mathrm{Med}^{k-1} \mathcal{F}} = \mathrm{Med}^k \mathcal{F} - \mathrm{FP}$.

Beweis.

1. $$\begin{aligned} \mathrm{FP}^{\mathrm{Med}^k \mathcal{F}} &\subseteq \mathrm{FS} \cdot \mathrm{Med}^k \mathcal{F} - \mathrm{FS} \cdot \mathrm{Med}^k \mathcal{F} && \text{wegen } 5.15 \\ &\subseteq \mathrm{FS}\,\mathrm{Med} \cdot \mathrm{Med}^{k-1} \mathcal{F} - \mathrm{FS}\,\mathrm{Med} \cdot \mathrm{Med}^{k-1} \mathcal{F} && \\ &\subseteq \mathrm{Med} \cdot \mathrm{FS}\,\mathrm{Med}^{k-1} \mathcal{F} - \mathrm{Med} \cdot \mathrm{FS}\,\mathrm{Med}^{k-1} \mathcal{F} && \text{wegen } 5.29 \\ &\subseteq \mathrm{Med}\,\mathrm{FP}^{\mathrm{Med}^{k-1} \mathcal{F}} - \mathrm{Med}\,\mathrm{FP}^{\mathrm{Med}^{k-1} \mathcal{F}} && \text{wegen } 5.10 \\ &\subseteq \mathrm{Med}^k \mathcal{F} - \mathrm{Med}^k \mathcal{F} && \text{wegen } 5.44, 2. \\ &\subseteq \mathrm{Med}^k \mathcal{F} + \mathrm{Med}^k \mathcal{F} - \mathrm{FP} && \text{wegen } 5.2 \\ &\subseteq \mathrm{FP}^{\mathrm{Med}^k \mathcal{F}} && \end{aligned}$$

2. Eine induktive Verallgemeinerung von Lemma 5.2, Teil 2(c), zeigt, daß unter den Voraussetzungen für alle k gilt: $\mathrm{Med}^k \mathcal{F} \subseteq \mathrm{FP} - \mathrm{Med}^k \mathcal{F}$. Die Behauptung folgt nun direkt aus 5.43.

□

Es ergeben sich also folgende Fixpunkte:

$$\mathrm{Med}^k \mathcal{F} \subseteq \mathrm{FS} \cdot \mathrm{Med}^k \mathcal{F} \subseteq \mathrm{FP}^{\mathrm{Med}^k \mathcal{F}} = \mathrm{FS} \cdot \mathrm{FP}^{\mathrm{Med}^k \mathcal{F}} \subseteq \mathrm{Med}^{k+1} \mathcal{F} - \mathrm{FP}$$

und

$$\mathrm{FS} \cdot \Gamma_{\mathrm{Med}}(\mathcal{F}) - \mathrm{FP} = \Gamma_{\mathrm{Med}}(\mathcal{F}) - \mathrm{FP}.$$

Definieren wir für Funktionenklassen $\mathcal{F}$

$$0 \,\#\, \mathrm{P}^{\mathcal{F}} =_{\mathrm{def}} \mathcal{F} \text{ und } (i+1) \,\#\, \mathrm{P}^{\mathcal{F}} =_{\mathrm{def}} \#\, \mathrm{P}^{i \,\#\, \mathrm{P}^{\mathcal{F}}} \text{ für } i \geq 0,$$

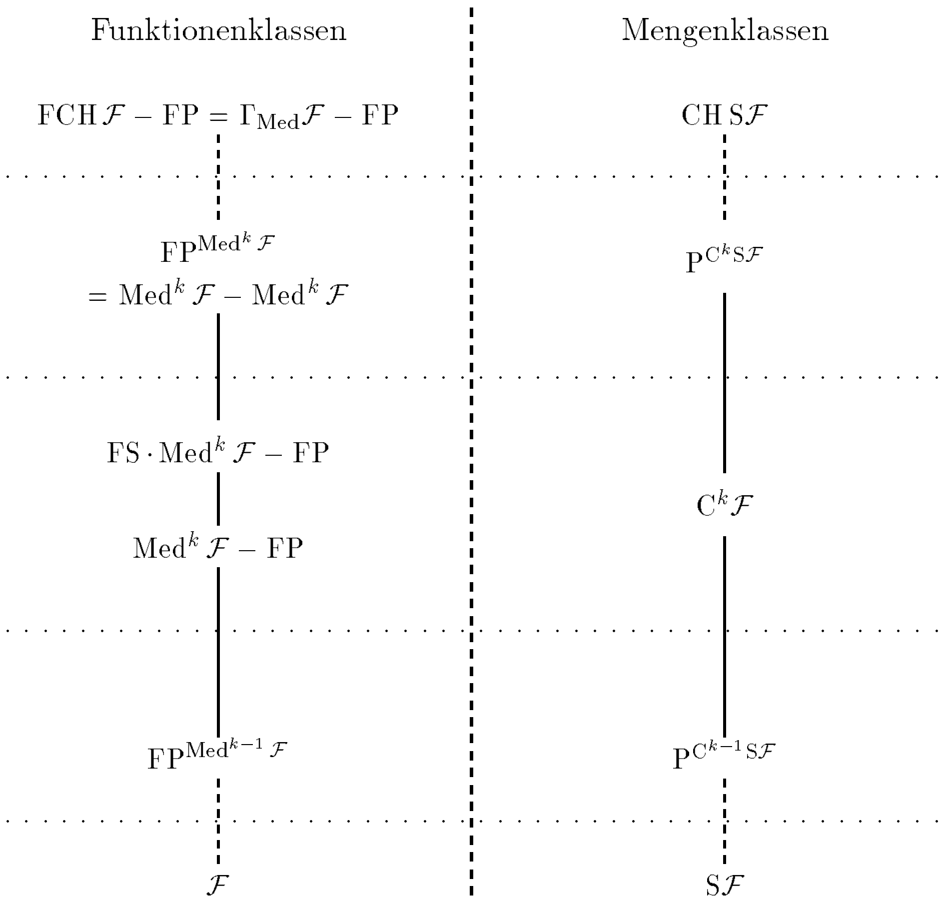

Abbildung 5.3: Die Med-Hierarchie

sowie $\mathrm{FCH} \cdot \mathcal{F} =_{\mathrm{def}} \bigcup_{k \geq 0} k \,\#\, \mathrm{P}^{\mathcal{F}}$, so gilt bezogen auf den letzten Fixpunkt folgendes:

5.45 Satz. *Sei $\mathcal{F}$ eine PFO und sei $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$. Dann gilt:*

$$\mathrm{F} \cdot \mathrm{CH} \cdot \mathrm{S}\mathcal{F} = \mathrm{FCH} \cdot \mathcal{F} - \mathrm{FP} = \Gamma_{\mathrm{Med}}(\mathcal{F}) - \mathrm{FP}.$$

Beweis. Wir zeigen per Induktion, daß für alle $k \geq 0$ gilt:

$$k \,\#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP} \subseteq \mathrm{FS} \cdot \mathrm{Med}^k \mathcal{F} \subseteq \mathrm{FP}^{k \,\#\, \mathrm{P}^{\mathcal{F}}} \subseteq (k+1) \,\#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP}.$$

Daraus folgt dann direkt

$$\bigcup_{k \geq 0} k \,\#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP} = \bigcup_{k \geq 0} \mathrm{Med}^k \mathcal{F} - \mathrm{FP} = \Gamma_{\mathrm{Med}}(\mathcal{F}) - \mathrm{FP}.$$

$k = 0$: $0 \,\#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP} = \mathcal{F} - \mathrm{FP} \subseteq \mathrm{FS}\mathcal{F} \subseteq \mathrm{FP}^{\mathcal{F}} \subseteq \#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP} = 1 \,\#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP}$.

$k-1 \to k$: Aus 5.28, 5.44 und der Induktionsvoraussetzung folgt:

$$\begin{aligned}
k \,\#\, \mathrm{P}^{\mathcal{F}} &\subseteq \#\, \mathrm{P}^{(k-1) \,\#\, \mathrm{P}^{\mathcal{F}}} \\
&\subseteq \mathrm{FS}\,\mathrm{Med}\,\mathrm{FP}^{(k-1) \,\#\, \mathrm{P}^{\mathcal{F}}} \\
&\subseteq \mathrm{FS}\,\mathrm{Med}\,\mathrm{FP}^{\mathrm{Med}^{k-1} \mathcal{F}} \\
&\subseteq \mathrm{FS}\,\mathrm{Med}^k \mathcal{F} - \mathrm{FP} \\
&\subseteq \mathrm{FP}^{\mathrm{Med}^k \mathcal{F} - \mathrm{FP}} \\
&\subseteq \#\, \mathrm{P}^{k \,\#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP}} - \mathrm{FP} \\
&\subseteq (k+1) \,\#\, \mathrm{P}^{\mathcal{F}} - \mathrm{FP}
\end{aligned}$$

□

Die Resultate dieses Abschnitts bezogen auf die Med-Hierarchie (unter den Voraussetzungen von Satz 5.44) werden in Bild 5.3 zusammengefaßt. Alle dort angegebenen Funktionenklassen, außer $\mathrm{Med}^k \mathcal{F}$, sind Fixpunkte von FS. Alle Funktionenklassen zwischen zwei gestrichelten Linien werden in die gleiche Mengenklasse auf der rechten Seite transformiert. Bei der Transformation in die umgekehrte Richtung erhält man als Resultat die obere der Klassen zwischen den zwei gestrichelten Linien.

5.6. Reduktionen

Wir werden uns nun im letzten Abschnitt dieses Kapitels kurz erneut dem in Kapitel 3 eingeführten Reduktionsbegriff zwischen Funktionen zuwenden und Satz 3.42 verallgemeinern und eine Umkehrung angeben.

5.46 Satz. *Sei $\mathcal{F}$ eine PFO. Hat $\mathcal{F}$ eine vollständige Funktion unter $\leq_m^{\mathrm{FP}}$-Reduktionen, so hat $\mathrm{S} \cdot \mathcal{F}$ eine $\leq_m^{\mathrm{P}}$-vollständige Menge.*

Beweis. Offensichtliche Verallgemeinerung des Beweises von 3.42. □

5.47 Satz. *Sei $\mathcal{F}$ eine PFO. Hat $\mathrm{S}\cdot\mathcal{F}$ eine $\leq_m^{\mathrm{P}}$-vollständige Menge, so hat $\mathrm{FS}\cdot\mathcal{F}$ eine $\leq_m^{\mathrm{FP}}$-vollständige Funktion.*

Beweis. Sei A vollständig für $\mathrm{S}\mathcal{F}$ unter $\leq_m^{\mathrm{P}}$-Reduktionen. Da $A \in \mathrm{S}\mathcal{F}$, existieren $f \in \mathcal{F}, g \in \mathrm{FP}$, so daß $x \in A \iff f(x) \geq g(x)$. Dann ist jedoch $A \leq_m^{\mathrm{P}} \mathrm{proj}(f)$, also ist $U =_{\mathrm{def}} \mathrm{proj}(f)$ vollständig für $\mathrm{S}\mathcal{F}$.

Sei $M_1, M_2, M_3, \ldots$ eine Aufzählung aller deterministischen Polynomialzeit-Turingmaschinen. Dann existiert eine Funktion $\hat{g} \in \mathrm{FP}$, so daß $\hat{g}(z, i, 2^t)$ gleich der Ausgabe der Maschine M_i bei Eingabe z nach t Schritten ist ($z \in \mathbb{Z}^k$ für ein $k \in \mathbb{N}$).

Definiere $\hat{U} =_{\mathrm{def}} \{\, (z, i, s) \mid \hat{g}(z, i, s) \in U \,\}$. Offensichtlich sind $\hat{U}$ und U many-one-äquivalent.

Definiere

$$\begin{aligned} &\hat{h}(x, i_1, j_1, i_2, j_2, i_3, j_3) \\ &\quad =_{\mathrm{def}} \max\{\, y \mid \hat{g}(x, i_1, j_i) \leq y \leq \hat{g}(x, i_2, j_2) \wedge ((x, y), i_3, j_3) \in \hat{U} \,\}. \end{aligned}$$

Dann ist $\hat{h} \in \mathrm{FS}\mathcal{F}$. Wir behaupten, daß $\hat{h}$ vollständig für $\mathrm{FS}\mathcal{F}$ unter $\leq_m^{\mathrm{FP}}$ ist. Sei dazu $f \in \mathrm{FS}\mathcal{F}$ beliebig,

$$f(x) = \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge (x, y) \in B \,\}$$

für $g_1, g_2 \in \mathrm{FP}$ und $B \in \mathrm{S}\mathcal{F}$. Sei $B \leq_m^{\mathrm{P}} U$ vermöge $g' \in \mathrm{FP}$. Dann ist

$$f(x) = \max\{\, y \mid g_1(x) \leq y \leq g_2(x) \wedge g'(x, y) \in U \,\}.$$

Es werde g' berechnet von der Maschine M_{i_3} in Zeit t_3 (oBdA hängt t_3 nur vom ersten Argument x ab), g_1 von M_{i_1} in Zeit t_1 und g_2 von M_{i_2} in Zeit t_2. Dann ist

$$f(x) = \max\{\, y \mid \hat{g}(x, i_1, 2^{t_1(x)}) \leq y \leq \hat{g}(x, i_2, 2^{t_2(x)}) \wedge (x, y, i_3, 2^{t_3(x)} \in \hat{U} \,\}.$$

Also ist $f \leq_m^{\mathrm{FP}} \hat{h}$ vermöge der Funktion

$$x \mapsto (x, i_1, 2^{t_1(x)}, i_2, 2^{t_2(x)}, i_3, 2^{t_3(x)}).$$

□

In [GaKrRa93] wird die These aufgestellt, daß jedes NP-vollständige Problem zu einer Opt P-vollständigen Funktion „erweitert" werden kann. Die Autoren begründen ihre These, indem sie für vierzig Probleme aus [GaJo79] entsprechende Funktionen angeben, die für Opt P unter (einer gewissen Verschärfung von) metrischen Reduktionen vollständig sind.

Unser Satz 5.47 beweist ein interessantes Pendant: Es ist unter sehr allgemeinen Voraussetzungen stets möglich, aus der Existenz eines vollständigen Problems für eine Mengenklasse auf die Existenz eines vollständigen Problems für die zugehörige Funktionenklasse zu schließen.

6

Zählfunktionen

In diesem Kapitel werden wir eine zweite „Kategorie" von Funktionenklassen untersuchen, die *Zählfunktionen*. Typische Funktionenklassen, an die wir dabei denken, sind $\#\mathrm{P}$, span-P und Gap-P. Wir führen zunächst den Begriff „p-fundierte Klasse von Zählfunktionen (PFZ)" ein und geben typische Vertreter dieser Funktionenkategorie an. Es stellt sich heraus, daß zum Beispiel für APKs $\mathcal{K}$ und PFOs $\mathcal{F}$ stets die Klassen $\#\mathcal{K}$, $\#\mathrm{S}\mathcal{F}$ und $\mathrm{Sum}\,\mathcal{F} - \mathrm{FP}$ (für den Sum-Operator siehe Abschnitt 6.2) PFZs sind. Danach geben wir eine Reihe von interessanten Fixpunktresultaten (ähnlich denen aus dem vorigen Kapitel) für die eben erwähnten Klassen an und untersuchen schließlich die Hierarchie der Zählfunktionen über allgemeinen PFOs oder PFZs.

6.1. P-fundierte Klassen von Zählfunktionen

Wir geben zunächst ähnlich wie in Definition 5.4 eine Reihe von Axiomen an. Eine Klasse von Zählfunktionen sollte zunächst sicherlich auch die Bedingungen 1 bis 5 aus Definition 5.4, die eher technischer Natur sind, erfüllen. Darüberhinaus stellen wir drei weitere Anforderungen, die für $\#\mathrm{P}$ in [BeGiHe90] und für Gap-P in [FeFoKu91] bewiesen werden, nämlich Abschluß unter exponentieller Summation, polynomiellem Produkt und polynomieller Auswahl. Ein Blick in die Literatur zeigt, daß fast alle Resultate im Kontext von Zählklassen (siehe z. B. [KSTT92, BeGiHe90, Her90, FeFoKu91, BeReSp90]) von genau diesen Eigenschaften der untersuchten Klassen abhängen.

Wir werden also zu folgender Definition geführt:

6.1 Definition. Eine Funktionenklasse $\mathcal{F}$ ist eine *p-fundierte Klasse von Zählfunktionen (PFZ)*, falls die folgenden Bedingungen erfüllt sind:

1. $\mathcal{F}$ ist polynomiall längenbeschränkt, enthält die Identitätsfunktion und ist abgeschlossen unter Komposition mit FP_+-Funktionen und Definition durch Fallunterscheidung.

2. Ist $f \in \mathcal{F}$, $g \in \mathrm{FP}$, so ist folgende Funktion h ein Element von $\mathcal{F}$:
$$h(x) = \sum_{0 \leq y \leq g(x)} f(x, y)$$
(*Abschluß unter exponentieller Summation*)

3. Ist $f \in \mathcal{F}$, $g \in \mathrm{FP}$, wobei $g(x) \leq p(|x|)$ für ein $p \in \mathrm{Pol}$, so ist folgende Funktion h ein Element von $\mathcal{F}$:
$$h(x) = \prod_{0 \leq y \leq g(x)} f(x, y)$$
(*Abschluß unter polynomieller Multiplikation*)

4. Ist $f \in \mathcal{F}$, $g \in \mathrm{FP}$, wobei $g(x) \leq p(|x|)$ für ein $p \in \mathrm{Pol}$, so ist folgende Funktion h ein Element von $\mathcal{F}$:
$$h(x) = \binom{f(x)}{g(x)}$$
(*Abschluß unter polynomieller Auswahl*)

Der Unterschied zwischen den Definitionen 5.4 und 6.1 liegt also darin, daß wir zum einen den Abschluß unter min-max-Operationen ersetzt haben durch drei andere Bedingungen. Zum anderen verlangen wir hier statt Abschluß unter Eingabetransformationen (wie in Definition 5.4) lediglich Abschluß unter Komposition mit FP_+-Funktionen. Der Grund ist der, daß es im Kontext von Zählfunktionen sinnvoll ist, Klassen von überall nicht-negativen Funktionen zu betrachten. Man beachte, daß die PFZ-Axiome trivialerweise Abschluß unter Addition und Multiplikation mit FP_+-Funktionen implizieren. Weiterhin beachte man, daß aus dem Abschluß einer Klasse unter Eingabetransformationen, Addition und Multiplikation mit FP_+-Funktionen sowie Summation direkt der strenge Abschluß unter Tupelbildung folgt.

6.2 Beobachtung. *Ist $\mathcal{F}$ eine PFZ, so ist $\mathcal{F}$ streng abgeschlossen unter Tupelbildung.*

Beweis. Der Term, mit dessen Hilfe die Kodierung $\langle \cdots \rangle$ definiert ist (vgl. Seite 14), kann mit den angegebenen Operationen direkt nachgebildet werden. □

Es stellt sich heraus, daß die Resultate aus [BeGiHe90, FeFoKu91] dahingehend verallgemeinert werden können, daß für abstrakte Polynomialzeit-Klassen stets $\#\mathcal{K}$ eine PFZ ist und darüberhinaus auch $\#\mathcal{K} - \#\mathcal{K}$ eine PFZ ist. Wenden wir uns zunächst $\#\mathcal{K}$ zu.

6.3 Satz. *Ist $\mathcal{K}$ eine APK, so ist $\#\mathcal{K}$ eine p-fundierte Klassen von Zählfunktionen.*

Beweis. Bedingung 1 ist offensichtlich erfüllt. Sei nun $f \in \#\mathcal{K}$, $f(x,y) = \#\{\, z \mid 0 \le z < g'(x) \wedge (x,y,z) \in A \,\}$ für $g' \in \mathrm{FP}$, $A \in \mathcal{K}$, und sei $g \in \mathrm{FP}$. Dann gilt:

$$\begin{aligned}\sum_{y<g(x)} f(x,y) &= \sum_{y<g(x)} \#\{\, z \mid 0 \le z < g'(x) \wedge (x,y,z) \in A \,\} \\ &= \#\{\, u \mid u = \langle z,y\rangle_{g'(x)}, 0 \le z < g'(x), 0 \le y < g(x) \\ &\qquad \wedge (x,y,z) \in A \,\};\end{aligned}$$

also ist $\#\mathcal{K}$ abgeschlossen unter exponentieller Summation.

Sei nun $g(x)$ beschränkt durch ein Polynom in $|x|$. Dann gilt:

$$\begin{aligned}\prod_{y<g(x)} f(x,y) &= \prod_{y<g(x)} \#\{\, z \mid 0 < z \le g'(x) \wedge (x,y,z) \in A \,\} \\ &= \#\{\, u \mid u = \langle z_0, z_1, \ldots, z_{g(x)-1}\rangle_{g'(x)} \wedge \\ &\qquad \bigwedge_{i=0}^{g(x)-1} (0 \le z_i < g'(x) \wedge (x,i,z) \in A) \,\};\end{aligned}$$

also ist $\#\mathcal{K}$ abgeschlossen unter polynomieller Multiplikation.

Sei nun $f \in \#\mathcal{K}$, $f(x) = \#\{\, y \mid 0 \le y < g'(x) \wedge (x,y) \in A \,\}$ für $g' \in \mathrm{FP}$, $A \in \mathcal{K}$, und sei g wie oben. Dann gilt:

$$\begin{aligned}\binom{f(x)}{g(x)} &= \#\{\, u \mid u = \langle y_0, y_1, \ldots, y_{g(x)-1}\rangle_{g(x)} \wedge \\ &\qquad \bigwedge_{i=0}^{g(x)-1} (0 \le y_i < g'(x) \wedge (x,y_i) \in A) \\ &\qquad \wedge y_0 < y_1 < \cdots < y_{g(x)} \,\};\end{aligned}$$

also ist $\#\mathcal{K}$ abgeschlossen unter polynomieller Auswahl. □

6.4 Korollar. *Ist $\mathcal{F}$ eine SPFO, so ist $\# \cdot \mathrm{S}\mathcal{F}$ eine PFZ.*

Kommen wir nun zu der Differenzklasse $\#\mathcal{K} - \#\mathcal{K}$. Wir beobachten zunächst einige einfache Eigenschaften:

6.5 Beobachtung. *Sei $\mathcal{K}$ eine APK. Dann gilt:*

1. $\#\mathcal{K} \subseteq \mathrm{FP} - \#\,\text{co-}\mathcal{K}$.

2. $\#\mathcal{K} - \#\mathcal{K} = \#\,\text{co-}\mathcal{K} - \#\,\text{co-}\mathcal{K} = \#\mathcal{K} + \#\,\text{co-}\mathcal{K}$.

Beweis.

1. Sei $f(x) = \#\{\, y \mid 0 \le y < g(x) \wedge (x,y) \in A \,\}$ für $g \in \mathrm{FP}$, $A \in \mathcal{K}$. Dann ist offensichtlich $f(x) = g(x) - \#\{\, y \mid 0 \le y < g(x) \wedge (x,y) \notin A \,\}$.

2. Direkte Folgerung aus Punkt 1.

□

6.6 Beobachtung. *Sei $\mathcal{K}$ eine APK, die unter Komplementbildung abgeschlossen ist. Dann gilt:*

1. $\#\mathcal{K} \subseteq \mathrm{FP} - \#\mathcal{K}$.
2. $\#\mathcal{K} - \#\mathcal{K} = \#\mathcal{K} - \mathrm{FP} = \mathrm{FP} - \#\mathcal{K}$.

6.7 Lemma. *Ist $\mathcal{F}$ eine PFZ, so ist auch $\mathcal{F} - \mathcal{F}$ eine PFZ.*

Beweis. Daß die Bedingungen 1 und 2 erfüllt sind, ist offensichtlich.

Seien $f, f' \in \mathcal{F}$, $g \in \mathrm{FP}$, wobei $g(x)$ durch ein Polynom in $|x|$ beschränkt ist. Dann kann offensichtlich der Term $\prod_{y \leq g(x)}(f(x,y) - f'(x,y))$ durch eine Summe polynomieller Produkte ausgedrückt werden, also ist $\mathcal{F} - \mathcal{F}$ abgeschlossen unter polynomialler Multiplikation.

Um zu zeigen, daß $\mathcal{F} - \mathcal{F}$ abgeschlossen unter polynomieller Auswahl ist, müssen wir nun also noch zeigen, daß die Funktion

$$h(x) =_{\mathrm{def}} \binom{f(x) - f'(x)}{g(x)}$$

ein Element von $\mathcal{F} - \mathcal{F}$ ist. Wir verwenden dazu folgende Beziehung [FeFoKu91, Lemma 3.7]: Für $r, j, k \in \mathbb{Z}$, $k \geq 0$ gilt:

$$\binom{j}{k} = (-1)^k \sum_{i=0}^{k} (-1)^i \binom{r+j+1}{k-i} \binom{r+i}{i}.$$

Wählen wir nun $r =_{\mathrm{def}} f'(x)$, $j =_{\mathrm{def}} f(x) - f'(x)$, $k =_{\mathrm{def}} g(x)$, so ergibt sich:

$$\binom{f(x) - f'(x)}{g(x)} = (-1)^{g(x)} \sum_{i=0}^{g(x)} (-1)^i \binom{f(x)+1}{g(x)-i} \binom{f'(x)+i}{i};$$

dieser Term zeigt, daß $h \in \mathcal{F} - \mathcal{F}$. □

6.8 Korollar.

1. *Ist $\mathcal{K}$ eine APK, so ist $\#\mathcal{K} - \#\mathcal{K}$ eine PFZ.*
2. *Ist $\mathcal{F}$ eine SPFO, so ist $\# \cdot \mathrm{S}\mathcal{F} - \# \cdot \mathrm{S}\mathcal{F}$ eine PFZ.*

6.9 Korollar.

1. *Ist $\mathcal{K}$ eine APK, die unter Komplementbildung abgeschlossen ist, so ist $\#\mathcal{K} - \mathrm{FP}$ eine PFZ.*

2. *Ist $\mathcal{F}$ eine SPFO, für die $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$ gilt, so ist $\# \cdot \mathrm{S}\mathcal{F} - \mathrm{FP}$ eine PFZ.*

Wir bemerken noch folgende interessante Beziehung zwischen den Abschlußeigenschaften:

6.10 Beobachtung. *Sei $\mathcal{F}$ eine PFZ, für die $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$ gilt. Dann ist $\mathrm{S} \cdot \mathcal{F}$ eine APK.*

Beweis. Aus Tabelle 5.1 ergibt sich, daß unter den Voraussetzungen an $\mathcal{F}$ die Klasse $\mathrm{S}\mathcal{F}$ die Klasse P enthält und unter markierter Vereinigung sowie Komplement abgeschlossen ist. Der Abschluß unter konjunktiven Reduktionen ergibt sich nun durch eine wörtliche Übertragung des Beweises aus [BeReSp90]. Die dort konstruierten Funktionen sind Elemente von $\mathcal{F} - \mathcal{F}$. Klarerweise ist jedoch $\mathrm{S}(\mathcal{F} - \mathcal{F}) = \mathrm{S}(\mathcal{F} - \mathrm{FP}) = \mathrm{S} \cdot \mathcal{F}$. □

6.2. Der Summationsoperator

Wir untersuchen in diesem Abschnitt einen Operator, der PFOs unter bestimmten schwachen Voraussetzungen in PFZs transformiert. Wir werden sehen, daß die PFZs, die so gebildet werden, besonders angenehme Eigenschaften haben. Satz 5.15 erlaubt es uns schließlich auch in diesem Kontext, eine sehr interessant Schlußfolgerung anzugeben.

6.11 Definition. Es sei $\mathcal{F}$ eine Funktionenklasse. Dann ist $h \in \mathrm{Sum}\,\mathcal{F}$ genau dann, wenn Funktionen $f \in \mathcal{F}$, $g \in \mathrm{FP}$ existieren, so daß

$$h(x) = \sum_{0 \leq y \leq g(x)} f(x, y).$$

Der Summationsoperator hat einige angenehme Eigenschaften, die denen der Optimierungsoperatoren, die wir in Abschnitt 5.1 untersuchten, ähneln.

6.12 Lemma.

1. *Ist $\mathcal{F}$ eine Funktionenklasse mit der Eigenschaft $\mathcal{F} + \mathrm{FP}_+ \subseteq \mathcal{F}$, so gilt:*
   (a) $\mathrm{Sum}(\mathcal{F} - \mathrm{FP}) = \mathrm{Sum}\,\mathcal{F} - \mathrm{FP}$.
   (b) $\mathrm{Sum}(-\mathcal{F}) = -\,\mathrm{Sum}\,\mathcal{F}$.
   (c) $\mathrm{Sum}(\mathrm{FP} - \mathcal{F}) = \mathrm{FP} - \mathrm{Sum}\,\mathcal{F}$.
2. *Ist $\mathcal{F}$ eine Funktionenklasse mit der Eigenschaft $\mathcal{F} \circ \mathrm{FP} \subseteq \mathcal{F}$, so gilt* $\mathrm{Sum}\,\mathrm{Sum}\,\mathcal{F} = \mathrm{Sum}\,\mathcal{F}$.

Beweis. Die Beweise verlaufen vollkommen analog zu den Beweisen der entsprechenden Resultate aus Abschnitt 5.1.

□

Es stellt sich nun heraus, daß der Summationsoperator angewandt auf PFOs in bestimmten Kontexten eine Zählklasse ergibt.

6.13 Satz. *Ist $\mathcal{F}$ eine PFO, so gilt:*

$$\mathrm{Sum}\,\mathcal{F} - \mathrm{FP} = \# \cdot \mathrm{S}\mathcal{F} - \mathrm{FP}.$$

Beweis.

$\subseteq$: Sei $h \in \mathrm{Sum}\,\mathcal{F}$, $h(x) = \sum_{0 \leq y < g(x)} f(x,y)$ für $f \in \mathcal{F}$, $g \in \mathrm{FP}$. Wähle $g_1, g_2 \in \mathrm{FP}$ mit $g_1(x) \leq f(x,y) \leq g_2(x)$ für $0 \leq y < g(x)$. Definiere $g_1'(x) =_{\mathrm{def}} g_1(x) \cdot \mathrm{sign}(g_1(x))$. Sicherlich ist $g_1' \in \mathrm{FP}_+$. Definiere $f' =_{\mathrm{def}} f + g_1'$. Sicherlich ist $f' \in \mathcal{F}$, $f' \geq 0$. Definiere $A \in \mathrm{S}\mathcal{F}$ durch $(x,y,z) \in A \iff f'(x,y) \geq z$. Dann gilt:

$$\begin{aligned}\textstyle\sum_{y<g(x)} f'(x,y) = \#\{\, u \mid u = \langle y,z\rangle_{g(x)}, 0 \leq y < g(x),\\ 0 \leq z \leq g_2(x) + g_1'(x) \wedge (x,y,z) \in A\,\}\end{aligned}$$

Da jedoch

$$h(x) = \sum_{y<g(x)} f'(x,y) - g(x) \cdot g_1'(x),$$

folgt $h \in \# \cdot \mathrm{S}\mathcal{F} - \mathrm{FP}$.

$\supseteq$: Wir zeigen, daß $\mathrm{char}(\mathrm{S} \cdot \mathcal{F}) \subseteq \mathcal{F} - \mathrm{FP}$. Daraus folgt dann direkt die behauptete Inklusion.

Sei $A \in \mathrm{S} \cdot \mathcal{F}$, $x \in A \iff f(x) \geq g(x)$ für $f \in \mathcal{F}$, $g \in \mathrm{FP}$. Dann ist offensichtlich

$$c_A(x) = \max\{g(x) - 1, \min\{g(x), f(x)\}\} - g(x) + 1;$$

also $c_A \in \mathcal{F} - \mathrm{FP}$.

□

6.14 Korollar. *Ist $\mathcal{F}$ eine SPFO mit der Eigenschaft $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$, so ist* $\mathrm{Sum}\,\mathcal{F} - \mathrm{FP}$ *eine PFZ.*

Beweis. Direkte Konsequenz aus 6.13 und 6.9. □

Der Summationsoperator verwischt also kleine Unterschiede zwischen Klassen, die das gleiche Bild unter S haben:

6.15 Korollar.

1. *Seien* $\mathcal{F}$ *und* $\mathcal{F}'$ *PFOs mit* $\mathrm{S}\mathcal{F} = \mathrm{S}\mathcal{F}'$. *Dann gilt:* $\mathrm{Sum}\,\mathcal{F} - \mathrm{FP} = \mathrm{Sum}\,\mathcal{F}' - \mathrm{FP}$.

2. *Sei* $\mathcal{F}$ *eine PFO. Dann gilt:* $\mathrm{Sum}\,\mathcal{F} - \mathrm{FP} = \mathrm{Sum}\cdot\mathrm{FS}\mathcal{F} - \mathrm{FP}$.

Beweis. Direkte Folgerung aus 6.13. □

Eine weitere Konsequenz aus 6.13 ist die, daß der Summationsoperator eine Komplexität hat, die der des Med-Operators vergleichbar ist.

6.16 Beobachtung. *Sei* $\mathcal{F}$ *eine PFO. Dann gilt:* $\mathrm{S}\cdot\mathrm{Med}\,\mathcal{F} = \mathrm{S}\cdot\mathrm{Sum}\,\mathcal{F}$.

Beweis. Für eine PFO gilt: $\mathrm{S}\cdot\mathrm{Med}\,\mathcal{F} = \mathrm{C}\cdot\mathrm{S}\mathcal{F} = \mathrm{S}\,\#\cdot\mathrm{S}\mathcal{F} = \mathrm{S}\,\mathrm{Sum}\,\mathcal{F}$. □

Eine direkte Verallgemeinerung des Beweises von $\#\mathrm{P} \subseteq \mathrm{Med}\,\mathrm{P}$ aus Kapitel 3 zeigt, daß allgemein für PFOs $\mathcal{F}$ gilt: $\#\,\mathrm{S}\mathcal{F} \subseteq \mathrm{Med}\,\mathcal{F} - \mathrm{FP}$. Damit erhalten wir allgemein für PFOs $\mathcal{F}$ die Inklusionen aus Abbildung 6.1.

Der Summationsoperator überführt offensichtlich die Klasse FP_+ in die Klasse $\#\,\mathrm{P}$ und die Klasse FP in die Klasse Gap-P. Diese Beziehungen können folgendermaßen verallgemeinert werden:

6.17 Korollar. *Ist* $\mathcal{F}$ *eine PFO, so gilt:*

$$\text{Gap-P}^{\mathcal{F}} = \mathrm{Sum}\,\mathcal{F} - \mathrm{Sum}\,\mathcal{F} = \#\,\mathrm{S}\mathcal{F} - \#\,\mathrm{S}\mathcal{F}.$$

Beweis. Aus Satz 5.15 und Korollar 6.15 folgt: $\text{Gap-P}^{\mathcal{F}} = \mathrm{Sum}\,\mathrm{FP}^{\mathcal{F}} = \mathrm{Sum}(\mathrm{FS}\mathcal{F} - \mathrm{FS}\mathcal{F}) = \mathrm{Sum}\,\mathrm{FS}\mathcal{F} - \mathrm{Sum}\,\mathrm{FS}\mathcal{F} = \mathrm{Sum}\,\mathcal{F} - \mathrm{Sum}\,\mathcal{F}$. Die zweite Gleichheit folgt daraus direkt. □

6.3. Transformationen

Wir werden in diesem Abschnitt zeigen, daß sich auch für Klassen von Zählfunktionen ein Paar von Konversionsoperatoren angeben läßt, deren Komposition eine Reihe interessanter Fixpunkte hat. Es handelt sich dabei um die Operatoren $\#$ für die Transformation von Mengenklassen in Funktionenklassen und U für die umgekehrte Transformation. Im Gegensatz zu den Operatoren F und

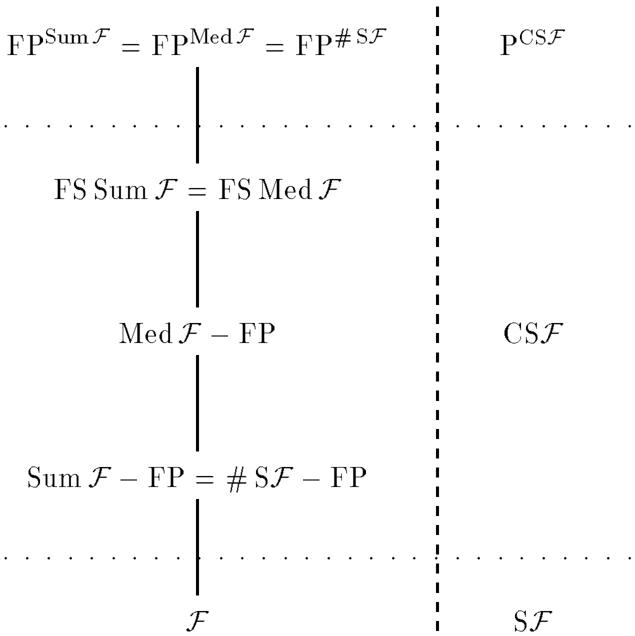

Abbildung 6.1: Der Summationsoperator

S aus dem letzten Kapitel haben diese Operatoren natürlich nicht die Eigenschaft, daß sie die Komplexität der Ausgangsklasse erhalten. Sicherlich sind die Klassen P und # P von stark unterschiedlicher Komplexität. Unser Interesse an dem Operatorenpaar #/U ist allein durch die interessanten Fixpunktresultate gerechtfertigt.

6.18 Satz. *Ist $\mathcal{K}$ eine Mengenklasse mit* $\mathrm{P} \subseteq \mathcal{K} = \mathcal{R}^{\mathrm{p}}_{m}(\mathcal{K})$, *so gilt:*

$$\mathcal{K} \subseteq \mathrm{U} \cdot \# \cdot \mathcal{K} \subseteq \exists \cdot \mathcal{K}.$$

Beweis. Sei $A \in \mathcal{K}$. Dann ist sicherlich $c_A \in \# \mathcal{K}$, denn es gilt

$$c_A(x) = \#\{\, y \mid 0 \leq y < 1 \wedge (x,y) \in A \times \{0\}\,\};$$

daraus folgt direkt $\mathcal{K} \subseteq \mathrm{U}\,\#\,\mathcal{K}$. $\mathrm{U}\,\#\,\mathcal{K} \subseteq \exists \mathcal{K}$ für alle Klassen $\mathcal{K}$ ist eine direkte Folgerung aus der Definition der beiden Operatoren. □

6.19 Korollar. *Ist $\mathcal{K}$ eine Mengenklasse, abgeschlossen unter Existenzquantifizierung, und ist* $\mathrm{P} \subseteq \mathcal{K} = \mathcal{R}^{\mathrm{p}}_{m}(\mathcal{K})$, *so gilt* $\mathrm{U} \cdot \# \cdot \mathcal{K} = \mathcal{K}$.

Wenden wir uns nun dem Kompositionsoperator # U zu. Wir geben zunächst eine allgemeine obere Schranke für seine Komplexität an.

6.20 Lemma. *Sei $\mathcal{F}$ eine Funktionenklasse mit* $\mathcal{F} + \mathrm{FP}_{+} \subseteq \mathcal{F}$. *Dann gilt:*

1. $\#\,\mathrm{U}\mathcal{F} \subseteq \mathrm{Sum}\,\mathcal{F}$.

2. $\#\,\mathrm{U}(\mathcal{F} - \mathrm{FP}) \subseteq \mathrm{Sum}\,\mathcal{F} - \mathrm{FP}$.

Beweis.

1. Sei $h \in \#\,\mathrm{U} \cdot \mathcal{F}$, $h(x) = \#\{\, y \mid 0 \leq y < g(x) \wedge (x,y) \in A\,\}$ für $A \in \mathrm{U}\mathcal{F}$, $g \in \mathrm{FP}$. Dann ist $c_A \in \mathcal{F}$. Also gilt:

$$h(x) = \sum_{y \leq g(x)} c_A(x,y).$$

   Daraus folgt $h \in \mathrm{Sum}\,\mathcal{F}$.

2. Folgt aus Punkt 1 und Lemma 6.12, Punkt 1(a).

□

Wir beweisen als nächstes, daß Zählklassen der Form $\#\mathcal{K}$ mit nur sehr schwachen Voraussetzungen an $\mathcal{K}$ stets Fixpunkte von $\#\,\mathrm{U}$ sind.

6.21 Satz. *Ist $\mathcal{K}$ eine Mengenklasse mit $\mathrm{P} \subseteq \mathcal{K} = \mathcal{R}^{\mathrm{p}}_{m}(\mathcal{K})$, so gilt:*

1. $\#\,\mathrm{U} \cdot \#\mathcal{K} = \#\mathcal{K}$.
2. $\#\,\mathrm{U}(\#\mathcal{K} - \mathrm{FP}) - \mathrm{FP} = \#\mathcal{K} - \mathrm{FP}$.

Beweis. In beiden Punkten gilt:

$\supseteq$: Folgt aus Satz 6.18.

$\subseteq$: Folgt aus Lemma 6.20 und dem Abschluß der Klassen $\#\mathcal{K}$ und $\#\mathcal{K} - \mathrm{FP}$ unter exponentieller Summation und Addition von FP_+-Funktionen.

□

Es ergeben sich direkt folgende Korollare (unter Berücksichtigung von Tabelle 5.1, Beobachtung 6.6 und Satz 6.13):

6.22 Korollar.

1. *Ist $\mathcal{K}$ eine Mengenklasse mit $\mathrm{P} \subseteq \mathcal{K} = \mathcal{R}^{\mathrm{p}}_{m}(\mathcal{K}) = \text{co-}\mathcal{K}$, so ist $\#\mathcal{K} - \#\mathcal{K}$ ein Fixpunkt von $\#\,\mathrm{U}(\cdot) - \mathrm{FP}$.*
2. *Ist $\mathcal{F}$ eine PFO, so ist $\#\,\mathrm{U} \cdot \#\,\mathrm{S}\mathcal{F} = \#\,\mathrm{S}\mathcal{F}$ und $\#\,\mathrm{U}(\#\,\mathrm{S}\mathcal{F} - \mathrm{FP}) - \mathrm{FP} = \#\,\mathrm{U}(\mathrm{Sum}\,\mathcal{F} - \mathrm{FP}) - \mathrm{FP} = \#\,\mathrm{S}\mathcal{F} - \mathrm{FP} = \mathrm{Sum}\,\mathcal{F} - \mathrm{FP}$.*

6.4. Die Hierarchie der Zählfunktionen

Als letztes wenden wir uns in diesem Kapitel relativierten Versionen der Hierarchie der Zählfunktionen zu und geben eine interessante algebraische Charakterisierung von Klassen dieser Form an.

6.23 Lemma. *Ist $\mathcal{F}$ eine PFO oder eine PFZ, so ist*

$$\mathrm{FP}^{\mathcal{F}}_{+} \subseteq \mathrm{Sum}(\mathcal{F} \dot{-} \mathcal{F}).$$

Beweis. Sei $f \in \mathrm{FP}^{h}$, $h \in \mathcal{F}$. Wähle wie im Beweis von Lemma 5.39 Funktionen g', g_M und $\hat{h}$. Beachte, daß sich auch für PFZs ergibt, daß $g', g_M \in \mathrm{FP}$ und $\hat{h} \in \mathcal{F}$.

Setze $t(a,b) =_{\mathrm{def}} (\min(a,b)+1) \dot{-} \max(a,b)$ im Falle einer PFO und $t(a,b) =_{\mathrm{def}} (2ab+1) \dot{-} (a^2+b^2)$ im Falle einer PFZ. Offenbar gilt $t(a,b) = 1 \iff a = b$ sowie $t(a,b) = 0 \iff a \neq b$ für $a, b \geq 0$. Dann folgt:

$$f(x) = \sum_{y \text{ wie in } 5.39} t(\hat{h}(x,y), y) \cdot g_M(x,y).$$

Also ist $h \in \mathrm{Sum}(\mathcal{F} \dot{-} \mathcal{F})$. □

Es ergeben sich folgende Konsequenzen:

6.24 Korollar. *Ist $\mathcal{F}$ eine PFO oder eine PFZ, so gilt:*

1. $\#\,\mathrm{P}^{\mathcal{F}} \subseteq \mathrm{Sum}(\mathcal{F} \dot{-} \mathcal{F})$.
2. $\mathrm{FCH} \cdot \mathcal{F} \subseteq \Gamma_{\mathrm{Sum},\dot{-}}(\mathcal{F})$.
3. $\#\,\mathrm{P}^{\mathcal{F}} - \mathrm{FP} = \mathrm{Sum}(\mathcal{F} \dot{-} \mathcal{F}) - \mathrm{FP}$.
4. $\mathrm{FCH} \cdot \mathcal{F} - \mathrm{FP} = \Gamma_{\mathrm{Sum},\dot{-}}(\mathcal{F}) - \mathrm{FP}$.

Besteht $\mathcal{F}$ nur aus nicht-negativen Funktionen, so werden auch die beiden Inklusionen zur Gleichheit.

Beweis. Aussage 1 ist eine offensichtliche Folgerung aus Lemma 6.23 und Lemma 6.12. Aussage 2 ergibt sich aus Lemma 6.23 unter Berücksichtigung der Tatsache, daß für eine PFZ $\mathcal{F}$ alle Klassen der Hierarchie der Zählfunktionen über $\mathcal{F}$ ebenfalls PFZs sind. Da für alle Orakel X gilt, daß $\mathrm{FP}^X = \mathrm{FP}^X_+ - \mathrm{FP}$, ergeben sich die Aussagen 3 und 4 aus $\mathcal{F} \subseteq \mathcal{F} \dot{-} \mathcal{F} \subseteq \mathrm{FP}^{\mathcal{F}} \subseteq \mathrm{FP}^{\mathcal{F}}_+ - \mathrm{FP} \subseteq \text{Gap-P}^{\mathcal{F}} = \#\,\mathrm{P}^{\mathcal{F}} - \mathrm{FP}$. □

7

Folgerungen

Wir werden in diesem Kapitel die allgemeinen Gleichungen über Funktionenklassen, die wir in den bisherigen Kapiteln erarbeitet haben, nutzen, um eine Reihe interessanter Folgerungen zu erhalten. Dabei werden wir einige Resultate aus jüngeren Arbeiten der Komplexitätstheorie stark verallgemeinern.

7.1 Satz. *Seien $\mathcal{F}_1$ und $\mathcal{F}_2$ Funktionenklassen mit der Eigenschaft, Fixpunkte von* $\mathrm{F} \cdot \mathrm{S}$ *zu sein. Dann gilt:*

$$\mathcal{F}_1 \subseteq \mathcal{F}_2 \iff \mathrm{S} \cdot \mathcal{F}_1 \subseteq \mathrm{S} \cdot \mathcal{F}_2.$$

Beweis. Direkte Folgerung aus der Monotonie der Operatoren. □

Für den Spezialfall der Counting-Hierarchie ergibt sich also, daß zwei ihrer Klassen genau dann zusammenfallen, wenn die entsprechenden Klassen der Min-Max-Med-Hierarchie über FP (ergänzt um ein führendes FS, falls der erste Operator ein Med ist) zusammenfallen.

7.2 Korollar. *Es seien Q_1, Q_2 Folgen von Operatoren aus* $(\mathrm{C}, \exists, \forall, \mathrm{FP}^{(\cdot)})^*$. *Es entstehen Q'_1 und Q'_2 aus Q_1 bzw. Q_2, indem jedes* C *durch* Med, *jedes* $\exists$ *durch* Max, *jedes* $\forall$ *durch* Min *und jedes* $\mathrm{FP}^{(\cdot)}$ *durch* $\mathrm{P}^{(\cdot)}$ *ersetzt und anschließend ein führendes* FS *eingeführt wird, falls der erste Operator ein* Med *ist. Dann gilt:*

$$Q'_1 \cdot \mathrm{FP} = Q'_2 \cdot \mathrm{FP} \iff Q_1 \cdot \mathrm{P} = Q_2 \cdot \mathrm{P}.$$

Es stellt sich jedoch heraus, daß wir ein leicht allgemeineres Resultat angeben können:

7.3 Satz. *Seien $\mathcal{F}_1$ und $\mathcal{F}_2$ Funktionenklassen, sei $\mathcal{F}_1$ abgeschlossen unter Eingabetransformationen und sei $\mathcal{F}_2$ ein Fixpunkt von* $\mathrm{F} \cdot \mathrm{S}$. *Dann gilt:*

$$\mathcal{F}_1 \subseteq \mathcal{F}_2 \iff \mathrm{S} \cdot \mathcal{F}_1 \subseteq \mathrm{S} \cdot \mathcal{F}_2.$$

Beweis. Die Implikation von links nach rechts ist trivial. Für die umgekehrte Richtung beachte man, daß wegen Satz 5.12 aus $\mathrm{S}\cdot\mathcal{F}_1 \subseteq \mathrm{S}\cdot\mathcal{F}_2$ folgendes folgt:

$$\mathcal{F}_1 \subseteq \mathrm{FS}\cdot\mathcal{F}_1 \subseteq \mathrm{FS}\cdot\mathcal{F}_2 \subseteq \mathcal{F}_2.$$

□

Es ergibt sich z. B. für die Polynomialzeithierarchie folgendes Resultat:

7.4 Korollar. *Für alle $j,k \geq 0$ gilt:* $\#\,\Sigma_j^p \subseteq \Sigma_k^p\cdot\mathrm{FP} \iff \mathrm{PP}^{\Sigma_j^p} \subseteq \Sigma_k^p$. *Insbesondere gilt:* $\#\,\mathrm{P} \subseteq \mathrm{Max}\,\mathrm{FP} \iff \mathrm{PP} = \mathrm{NP}$.

Man beachte, daß aus einer dieser Inklusionen sich stets der Kollaps der Polynomialzeithierarchie ergibt [Tod91].

Korollar 7.4 verallgemeinert ein Resultat aus [KöScTo89]. Dort wurde bereits der Spezialfall $j = 0, k = 1$ und eine Richtung der Äquivalenz für den Spezialfall $j = 1, k = 1$ bewiesen.

Im Kontext von Zählklassen mit Basisklassen aus der Polynomialzeithierarchie lassen sich zwei interessante absolute Resultate angeben.

In [KöScTo89] wurde bewiesen, daß sich jede Funktion aus $\#\,\mathrm{P}^{\#\,\mathrm{NP}}$ als Differenz zweier Funktionen aus span-P = $\#\,\mathrm{NP}$ schreiben läßt. Toran [Tor88] erweiterte diese Inklusion aus [KöScTo89] für höhere Stufen der Polynomialzeithierarchie. Wir können nun folgendes Pendant beweisen:

7.5 Korollar. *Für alle $k \geq 0$ gilt:*

$$\text{Gap-P}^{\Sigma_k^p} = \#\,\Sigma_k^p - \#\,\Sigma_k^p = \#\,\Pi_k^p - \#\,\Pi_k^p.$$

Beweis. Aus Korollar 6.17 folgt: $\text{Gap-P}^{\Sigma_k^p} = \text{Gap-P}^{\Sigma_k^p\cdot\mathrm{FP}} = \#\,\mathrm{S}\cdot\Sigma_k^p\mathrm{FP} - \#\,\mathrm{S}\cdot\Sigma_k^p\mathrm{FP} = \#\,\Sigma_k^p - \#\,\Sigma_k^p$. □

In Korollar 7.4 sahen wir, daß Zählklassen vermutlich nicht in den Klassen der Min-Max-Hierarchie enthalten sind. Umgekehrt gilt jedoch folgendes:

7.6 Korollar. *Für alle $k \geq 0$ gilt:* $\Sigma_k^p\cdot\mathrm{FP} \subseteq \#\,\Sigma_k^p - \mathrm{FP}$.

Beweis. Für alle Funktionenklassen, die abgeschlossen sind unter Eingabetransformationen, gilt $\mathcal{F} \subseteq \#\,\mathrm{S}\mathcal{F}$; denn eine Funktion f kann stets als Summation über die charakteristische Funktion der Projektion von f geschrieben werden, vgl. Beobachtung 5.11. □

Korollar 7.6 verallgemeinert ein Resultat aus [KöScTo89, Köb89]. Dort wurde schon der Spezialfall $k = 1$ bewiesen.

Ähnliche Resultate wie in Satz 7.1 lassen sich natürlich auch für die Fixpunkte des Operatorenpaars $\#/\mathrm{U}$ angeben.

7.7 Satz. *Seien $\mathcal{K}_1$ und $\mathcal{K}_2$ APKs. Dann gilt:*

1. $\#\,\mathcal{K}_1 = \#\,\mathcal{K}_2 \iff \mathrm{U}\cdot\mathcal{K}_1 = \mathrm{U}\cdot\mathcal{K}_2$.
2. $\#\,\mathcal{K}_1 - \mathrm{FP} = \#\,\mathcal{K}_2 - \mathrm{FP} \iff \mathrm{U}(\#\,\mathcal{K}_1 - \mathrm{FP}) = \mathrm{U}(\#\,\mathcal{K}_2 - \mathrm{FP})$.

Beweis.

1. Direkte Folgerung aus Satz 6.21.
2. Die Implikation von links nach rechts folgt aus der Monotonie von U. Die Implikation von rechts nach links ergibt sich, da mit Satz 6.21 folgt:

$$\#\,\mathcal{K}_1{-}\mathrm{FP} = \#\cdot\mathrm{U}(\#\,\mathcal{K}_1{-}\mathrm{FP}){-}\mathrm{FP} = \#\cdot\mathrm{U}(\#\,\mathcal{K}_2{-}\mathrm{FP}){-}\mathrm{FP} = \#\,\mathcal{K}_2{-}\mathrm{FP}.$$

□

Interessante Fälle ergeben sich erneut im Kontext der Polynomialzeithierarchie:

7.8 Korollar. *Für $k \geq 1$ gilt:*

1. (a) $\#\,\Delta^p_{k+1} = \#\,\Sigma^p_{k+1} \iff \mathrm{UP}^{\Sigma^p_k} = \Sigma^p_{k+1}$.
   (b) $\#\,\Sigma^p_k = \#\,\Delta^p_{k+1} \iff \Sigma^p_k = \mathrm{UP}^{\Sigma^p_k} \iff \mathrm{PH} = \Sigma^p_k$.
2. $\text{Gap-P}^{\Sigma^p_k} = \#\,\Sigma^p_{k+1} - \#\,\Sigma^p_{k+1} \iff \mathrm{XP}^{\Sigma^p_k} = \mathrm{XP}^{\Sigma^p_{k+1}}$.

Beweis.

1. (a) Setze in Satz 7.7 $\mathcal{K}_1 = \Delta^p_{k+1}$, $\mathcal{K}_2 = \Sigma^p_{k+1}$.
   (b) Setze in Satz 7.7 $\mathcal{K}_1 = \Sigma^p_k$, $\mathcal{K}_2 = \Delta^p_{k+1}$.
2. Setze in Satz 7.7 $\mathcal{K}_1 = \text{Gap-P}^{\Sigma^p_k}$, $\mathcal{K}_2 = \#\,\Sigma^p_{k+1} - \#\,\Sigma^p_{k+1} = \text{Gap-P}^{\Sigma^p_{k+1}}$. Satz 7.7 kann angewandt werden, da eine Relativierung eines Resultats aus [Sparta91] ergibt, daß für alle Orakel X gilt: $\#\,\mathrm{NP}^X - \#\,\mathrm{NP}^X = \#\,\mathrm{NP}^X - \mathrm{FP}$.

□

Punkt 1 des vorigen Resultats wurde bereits bewiesen in [Tor88].

Alle bisher angegebenen Resultate dieses Kapitels zeigten Äquivalenzen zu Gleichheiten von Funktionenklassen auf. Als nächstes wenden wir uns der Frage des Abschlusses von Funktionenklassen unter bestimmten Operationen zu.

7.9 Satz. *Sei $\mathcal{F}$ eine PFZ und enthalte $\mathcal{F}$ nur überall nicht-negative Funktionen. Dann sind die folgenden Aussagen äquivalent:*

1. *$\mathcal{F}$ ist abgeschlossen unter modifizierter Differenz.*
2. *$\mathcal{F}$ ist abgeschlossen unter jeder FP_+-Operation.*
3. $\mathrm{U} \cdot \mathcal{F} = \mathrm{CH} \cdot \mathrm{S}\mathcal{F}$.
4. $\mathcal{F} = \mathrm{FCH} \cdot \mathcal{F}$.

Beweis. Die Äquivalenz von 1. und 4. folgt direkt aus Korollar 6.24.

Weiterhin gilt: Ist $\mathcal{F} = \mathrm{FCH} \cdot \mathcal{F}$, so ist $\mathrm{U} \cdot \mathcal{F} = \mathrm{U} \cdot \mathrm{FCH} \cdot \mathcal{F} = \mathrm{CH} \cdot \mathrm{S}\mathcal{F}$. Daraus folgt dann mit Lemma 6.20 $\#\,\mathrm{U}\mathcal{F} \subseteq \mathcal{F} \subseteq \mathrm{FCH}\,\mathcal{F}\,\#\,\mathrm{CH}\,\mathrm{S}\mathcal{F} \subseteq \#\,\mathrm{U}\mathcal{F}$. Also gilt 4. $\Rightarrow$ 3. $\Rightarrow$ 4.

Um den Beweis zu beenden, genügt es, zu beobachten, daß offensichtlich 2. $\Rightarrow$ 1. und (da $\mathrm{FCH} \cdot \mathcal{F}$ unter FP_+-Operationen abgeschlossen ist) 4. $\Rightarrow$ 2. □

7.10 Korollar. *Für alle $k \geq 0$ gilt: $\#\,\Sigma_k^p$ ist abgeschlossen unter modifizierter Differenz genau dann, wenn $\mathrm{U} \cdot \Sigma_k^p = \mathrm{CH}$ genau dann, wenn $\#\,\Sigma_k^p = \mathrm{FCH}$.*

Korollar 7.10 verallgemeinert ein Resultat aus [OgHe93]. Dort wurden die Spezialfälle $k = 0$ ($\#\,\mathrm{P}$) und $k = 1$ (span-P) bewiesen. (Beachte, daß $\mathrm{U} \cdot \Sigma_k^p = \Sigma_k^p$ für $k \geq 1$.)

Lassen wir in den Ausgangsklassen auch Funktionen zu, die negative Werte annehmen dürfen, so ergibt sich:

7.11 Korollar. *Sei $\mathcal{F}$ eine PFZ. Dann sind die folgenden Aussagen äquivalent:*

1. *$\mathcal{F} - \mathrm{FP}$ ist abgeschlossen unter modifizierter Differenz.*
2. *$\mathcal{F} - \mathrm{FP}$ ist abgeschlossen unter jeder FP-Operation.*
3. $\mathrm{U}(\mathcal{F} - \mathrm{FP}) = \mathrm{CH} \cdot \mathrm{S}\mathcal{F}$.
4. $\mathcal{F} - \mathrm{FP} = \mathrm{FCH} \cdot \mathcal{F} - \mathrm{FP}$.

Beweis. Vollkommen analog zum Beweis von 7.9. □

7.12 Korollar. *Für alle $k \geq 0$ gilt: $\#\Sigma_k^p - \#\Sigma_k^p$ ist abgeschlossen unter modifizierter Differenz genau dann, wenn $\mathrm{XP}^{\Sigma_k^p} = \mathrm{CH}$ genau dann, wenn $\#\Sigma_k^p - \#\Sigma_k^p = \mathrm{FCH} - \mathrm{FP}$.*

Korollar 7.12 verallgemeinert ein Resultat aus [ThToWa93]. Dort wurde der Fall $k = 0$ unter Einschränkung auf positive Funktionen in Gap-P bewiesen.

7.13 Bemerkung. In Satz 7.9 (und analog in Korollar 7.11) kann die Reihe der äquivalenten Statements um Aussagen der Form „$\mathcal{F} - \mathrm{FP}$ ist abgeschlossen unter den Operationen O“ erweitert werden, falls die Operationen aus O in deterministischer Polynomialzeit berechnet werden können und modifizierte Subtraktion simulieren können. Beispielsweise könnte man in Satz 7.9 einfügen:

1(a) $\mathcal{F}$ ist abgeschlossen unter Maximierung und Subtraktion eingeschränkt auf nichtnegative Werte (d.h. $a - b$ ist nur dann definiert, falls $a, b \geq 0$, $a \geq b$).

1(b) $\mathcal{F}$ ist abgeschlossen unter Minimierung und Subtraktion eingeschränkt auf nichtnegative Werte.

Dies folgt daraus, daß trivialerweise $2 \Rightarrow$ 1(a), 1(b). Direkt aus der Definition von $\dot{-}$ folgt jedoch, daß 1(a), 1(b) $\Rightarrow$ (1). Beachte, daß wir es nur mit positiven Funktionen zu tun haben und daher die Fallunterscheidung in der Definition von $\dot{-}$ ignorieren können.

Modifizierte Subtraktion ist also (um es mit den Worten von Ogiwara und Hemachandra [OgHe93] auszudrücken) eine „harte“ Operation für Zählklassen. Abschluß von Zählklassen unter gewöhnlicher Subtraktion ist hingegen nichts außergewöhnliches (man denke nur an Gap-P). Für Optimierungsklassen ist jedoch schon die gewöhnliche Subtraktion hart. Aus Satz 5.15 folgt direkt, daß eine PFO $\mathcal{F}$, die ein Fixpunkt von FS ist, genau dann unter Subtraktion abgeschlossen ist, wenn $\mathcal{F} = \mathrm{FP}^{\mathcal{F}}$.

Aus Korollar 5.41 folgt jedoch noch mehr:

7.14 Satz. *Sei $\mathcal{F}$ eine PFO mit $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$ und sei $k \geq 1$. Dann sind die folgenden Aussagen äquivalent:*

1. *$\Sigma_k^p\mathcal{F} - \mathrm{FP}$ ist abgeschlossen unter Subtraktion.*
2. *$\Sigma_k^p\mathcal{F}$ ist abgeschlossen unter modifizierter Subtraktion und Subtraktion von* FP*-Funktionen.*
3. *$\Sigma_k^p\mathcal{F} - \mathrm{FP}$ ist abgeschlossen unter jeder* FP*-Operation.*

4. $\Sigma_k^p \cdot \mathrm{S}\mathcal{F} = \mathrm{PH} \cdot \mathrm{S}\mathcal{F}$.

5. $\Sigma_k^p \mathcal{F} - \mathrm{FP} = \mathrm{FPH} \cdot \mathcal{F}$.

6. $\Pi_k^p \mathcal{F} - \mathrm{FP}$ *ist abgeschlossen unter Subtraktion.*

7. $\Pi_k^p \mathcal{F}$ *ist abgeschlossen unter modifizierter Subtraktion und Subtraktion von* FP-*Funktionen.*

8. $\Pi_k^p \mathcal{F} - \mathrm{FP}$ *ist abgeschlossen unter jeder* FP-*Operation.*

9. $\Pi_k^p \cdot \mathrm{S}\mathcal{F} = \mathrm{PH} \cdot \mathrm{S}\mathcal{F}$.

10. $\Pi_k^p \mathcal{F} - \mathrm{FP} = \mathrm{FPH} \cdot \mathcal{F}$.

Beweis. 1. $\Leftrightarrow$ 5. folgt direkt aus 5.41. 4. $\Leftrightarrow$ 5. folgt direkt aus 7.1. Da $\mathrm{FPH} \cdot \mathcal{F}$ unter jeder FP-Operation abgeschlossen ist, folgt 3. $\Rightarrow$ 1. $\Rightarrow$ 5. $\Rightarrow$ 3. Gewöhnliche Subtraktion kann durch modifizierte Subtraktion und Subtraktion von FP-Funktionen leicht simuliert werden, also folgt 2. $\Rightarrow$ 1. $\Rightarrow$ 5. $\Rightarrow$ 2. Die Äquivalenz mit den Aussagen 6 bis 10 ist offensichtlich. $\square$

Satz 7.14 verallgemeinert ein Resultat aus [OgHe93]. Dort wurde unser Resultat für $\mathcal{F} = \mathrm{FP}$, $k = 1$ bewiesen.

7.15 Satz. *Sei $\mathcal{F}$ eine PFO mit $\mathcal{F} \subseteq \mathrm{FP} - \mathcal{F}$ und sei $k \geq 1$. Dann sind die folgenden Aussagen äquivalent:*

1. $\mathrm{Med}^k \mathcal{F} - \mathrm{FP}$ *ist abgeschlossen unter Subtraktion.*

2. $\mathrm{Med}^k \mathcal{F} - \mathrm{FP}$ *ist abgeschlossen unter Addition.*

3. $\mathrm{Med}^k \mathcal{F}$ *ist abgeschlossen unter modifizierter Subtraktion und Subtraktion von* FP-*Funktionen.*

4. $\mathrm{Med}^k \mathcal{F} - \mathrm{FP}$ *ist abgeschlossen unter jeder* FP-*Operation.*

5. $\mathrm{C}^k \cdot \mathrm{S}\mathcal{F}$ *ist abgeschlossen unter Turing-Reduktionen.*

Beweis. Direkte Folgerung aus Satz 5.44. $\square$

Index

Literatur

[AlWi90] E. ALLENDER, C. WILSON, Width-bounded reducibility and binary search over complexity classes; *Proceedings of the* 5^{th} *Structure in Complexity Theory Conference* (1990), pp. 122–129.

[BaDiGa88] J. L. BALCÁZAR, J. DÍAZ, J. GABARRÓ, *Structural Complexity I;* Springer (Berlin – Heidelberg – New York, 1988).

[BaDiGa90] J. L. BALCÁZAR, J. DÍAZ, J. GABARRÓ, *Structural Complexity II;* Springer (Berlin – Heidelberg – New York, 1990).

[Bei92] R. BEIGEL, Perceptrons, PP, and the polynomial time hierarchy; *Proceedings of the* 7^{th} *Structure in Complexity Theory Conference* (1992), pp. 14–19.

[BeGiHe90] R. BEIGEL, J. GILL, U. HERTRAMPF, Counting classes: thresholds, parity, mods, and fewness; *Proceedings of the* 7^{th} *Symposium on Theoretical Aspects of Computer Science* (1990), LNCS 415, pp. 49–57.

[BeReSp90] R. BEIGEL, N. REINGOLD, D. SPIELMAN, PP is closed under intersection; *Proceedings of the* 23^{rd} *Symposium on Theory of Computing* (1991), pp. 1–9.

[BuHa88] S. BUSS, L. HAY, On truth-table reducibility and the difference hierarchy over NP; *Proceedings of the* 3^{rd} *Structure in Complexity Theory Conference* (1988), pp. 224–233.

[Coo71] S. A. COOK, The complexity of theorem proving procedures; *Proceedings of the* 3^{rd} *Symposium on the Theory of Computing* (1971), pp. 151–158.

[FeFoKu91] S. FENNER, L. FORTNOW, S. KURTZ, Gap-definable counting classes; *Proceedings of the* 6^{th} *Structure in Complexity Theory Conference* (1991), pp. 30–42.

[FoRe91] L. FORTNOW, N. REINGOLD, PP is closed under truth-table reductions; *Proceedings of the* 6^{th} *Structure in Complexity Theory Conference* (1991), pp. 13–15.

[GaJo79] M. R. Garey, D. S. Johnson, *Computers and Intractability: A Guide to the Theory of* NP-*Completeness;* Freeman & Co. (New York, 1979).

[GaKrRa93] W. I. Gasarch, M. W. Krentel, K. J. Rappoport, Opt P as the normal behaviour of NP-complete problems; manuscript, 1993.

[Gil77] J. Gill, Computational complexity of probabilistic complexity classes; *SIAM Journal on Computing* **6** (1977), pp. 675–695.

[GiSeHo69] S. Ginsburg, S. Greibach, J. Hopcroft, *Studies in Abstract Families of Languages;* Memoir #87, American Mathematical Society (1960).

[Gre90] F. Green, An oracle separating $\oplus$P from $\mathrm{PP}^{\mathrm{PH}}$; *Proceedings of the* 5^{th} *Structure in Complexity Theory Conference* (1990), pp. 295–298.

[GKRTT92] F. Green, J. Köbler, K. W. Regan, T. Schwentick, J. Torán, The power of the middle bit of a # P function; submitted.

[Her90] U. Hertrampf, Relations among MOD-classes; *Theoretical Computer Science* **74** (1990), pp. 325–328.

[HLSVW93] U. Hertrampf, C. Lautemann, T. Schwentick, H. Vollmer, K. W. Wagner, On the power of polynomial time bit-reductions; *Proceedings of the* 8^{th} *Structure in Complexity Theory Conference* (1993), pp. 200–207.

[HoUl79] J. E. Hopcroft, J. D. Ullman, *Introduction to Automata Theory, Languages, and Computation,* Addison-Wesley Publishing Company (Reading, Mass., 1979).

[Kad87] J. Kadin, $\mathrm{P}^{\mathrm{NP}}[\log n]$ and Sparse Turing Complete Sets for NP; *Proceedings of the* 2^{nd} *Structure in Complexity Theory Conference* (1987), pp. 33–40.

[Köb89] J. Köbler, Strukturelle Komplexität von Anzahlproblemen, Dissertation, Fakultät für Informatik, Universität Stuttgart, 1989.

[KöScTo89] J. Köbler, U. Schöning, J. Torán, On counting and approximation; *Acta Informatica* **26** (1989), pp. 363–379.

[KöTo93] J. Köbler, S. Toda, On the power of generalized MOD-classes, *Proceedings of the* 8^{th} *Structure in Complexity Theory Conference* (1993), pp. 147–155.

[Kre88] M. W. Krentel, The complexity of optimization problems; *Journal of Computer and Systems Sciences* **36** (1988), pp. 490–509.

[Kre92] M. W. Krentel, Generalizations of Opt P to the polynomial hierarchy; *Theoretical Computer Science* **97** (1992), pp. 183–198.

[KSTT92] J. Köbler, U. Schöning, S. Toda, J. Torán, Turing machines with few accepting configurations and low sets for PP; *Journal of Computer and Systems Sciences* **44** (1992), pp. 272–286.

[Lad75] R. E. Ladner, The circuit value problem is log space complete for P; *SIGACT News* **7** (1975), pp. 18–20.

[Lau83] C. Lautemann, BPP and the polynomial hierarchy; *Information Processing Letters* **117** (1983), pp. 215–217.

[Li93] L. Li, The classes low for PP; manuscript, 1993.

[Ogi91] M. Ogiwara, Characterizing low levels of the polynomial-time hierarchy relative to $\mathrm{C}_{=}\mathrm{P}$ via metric turing machines; Department of Information Sciences, Tokyo Institute of Technology, Report C-101 (1991).

[OgHe93] M. Ogiwara, L. Hemachandra, A complexity theory for feasible closure properties; *Journal of Computer and System Sciences* **46** (1993), pp. 295–325.

[PaSt82] C. H. Papadimitriou, K. Steiglitz, *Combinatorial Optimization;* Prentice Hall (Englewood Cliffs, New Jersey, 1982).

[PaZa83] C. H. Papadimitriou, S. K. Zachos, Two remarks on the power of counting; 6^{th} *GI-Conference on Theoretical Computer Science* (1983), LNCS 145, pp. 269–275.

[Sch86] U. Schöning, *Complexity and Structure;* Springer (Berlin – Heidelberg – New York, 1986).

[Sim75] J. Simon, On Some Central Problems in Computational Complexity; Dissertation, Cornell University, 1975.

[Sip83] M. Sipser, A complexity theoretic approach to randomness; *Proceedings of the* 15^{rd} *Symposium on Theory of Computing* (1983), pp. 330–335.

[Sparta91] H. J. Burtschick, Notes of a seminar on complexity theory, Georgenthal, 1991.

[ThToWa93] T. THIERAUF, S. TODA, O. WATANABE, On closure properties of Gap-P; Department of Computer Science, Tokyo Institute of Technology, Report 93TR-0002 (1993).

[Tod90] S. TODA, The complexity of finding medians; *Proceedings of the* 31^{st} *Symposium on Foundations of Computer Science* (1990), pp. 778–787.

[Tod91] S. TODA, PP is as hard as the polynomial time hierarchy; *SIAM J. Comput.* **20** (1991), pp. 865–877.

[ToWa91] S. TODA, O. WATANABE, Polynomial time 1-Turing reductions from #PH to #P; *Theoretical Computer Science* **100** (1992), pp. 205–221.

[Tor88] J. TORÁN, Structural Properties of the Counting Hierarchies; Dissertation, Facultat d'Informàtica de Barcelona, 1988.

[Tor91] J. TORÁN, Complexity classes defined by counting quantifiers; *Journal of the ACM* **38** (1991), pp. 753–774.

[Val76] L. G. VALIANT, Relative complexity of checking and evaluation, *Information Processing Letters* **5** (1976), pp. 20–23.

[Val79] L. G. VALIANT, The complexity of computing the permanent; *Theoretical Computer Science* **8** (1979), pp. 189–201.

[Vol91] H. VOLLMER, The gap-language technique revisited; *Proceedings of the* 4^{th} *Computer Science Logic Conference*, LNCS 533 (1991), pp. 389–399.

[Vol93] H. VOLLMER, On different reducibility notions for function classes; Fachbereich Mathematik und Informatik, Universität Würzburg, Technischer Bericht Nr. 62 (1993), eingereicht.

[VoWa91a] H. VOLLMER, K. W. WAGNER, Classes of counting functions and complexity theoretic operators; Fachbereich Mathematik und Informatik, Universität Würzburg, Technischer Bericht Nr. 31 (1991).

[VoWa93a] H. VOLLMER, K. W. WAGNER, Complexity of functions versus complexity of sets; Fachbereich Mathematik und Informatik, Universität Würzburg, Technischer Bericht Nr. 35 (1993), eingereicht.

[VoWa93b] H. VOLLMER, K. W. WAGNER, The complexity of finding middle elements; Fachbereich Mathematik und Informatik, Universität Würzburg, Technischer Bericht Nr. 53 (1993), eingereicht.

[Wag86a] K. W. WAGNER, The complexity of combinatorial problems with succinct input representation; *Acta Informatica* **23** (1986), pp. 325—356.

[Wag86b] K. W. WAGNER, Some observations on the connection between counting and recursion; *Theoretical Computer Science* **47** (1986), pp. 131–147.

[Wag90] K. W. WAGNER, Bounded query classes; *SIAM J. Comput.* **19** (1990), pp. 833–846.

[WaWe86] K. W. WAGNER, G. WECHSUNG, *Computational Complexity;* Deutscher Verlag der Wissenschaften (Berlin, 1986).

[Wra77] C. WRATHALL, Complete sets and the polynomial-time hierarchy; *Theoretical Computer Science* **3** (1977), pp. 23–33.