Kurse der QED-Akademie 2016

(Stand: 22. August 2016)

Inhaltsverzeichnis

1 Algorithmische Komposition von Kontrapunkt im Palestrina-Stil

2 Typentheorie

3 Homotopietheorie

4 Einführung in die Galoistheorie

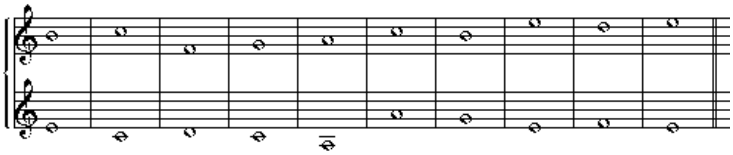
5 Kryptographie und Kryptoanalyse

1 Algorithmische Komposition von Kontrapunkt im Palestrina-Stil

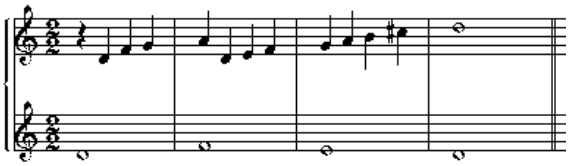
Wir werden gemeinsam ein C++14-Programm schreiben, das tolle, mehrstimmige Stücke erzeugt. Die Kompositionstechnik heißt Kontrapunkt (»punctus contra punctum« – »Note gegen Note«; sie bezeichnet eine »Gegenstimme« zu einer vorgegebenen Melodie) im Palestrina-Stil. Dies ist mindestens zweistimmige polyphone, d. h. mit eigenständigen Stimmen, Musik der Renaissance.

Das Programm ist im wesentlichen ein Backtracking-Algorithmus, und die meiste Zeit werden wir damit verbringen, die Kompositionsregeln zu programmieren, z. B.: welche Intervalle sind erlaubt, wie dürfen die Stimmen fortschreiten? Wenn jemand Lust hat, kann er das Programm auch noch multithreading-fähig machen (hierfür sind keine Musiktheoriekenntnisse vonnöten).

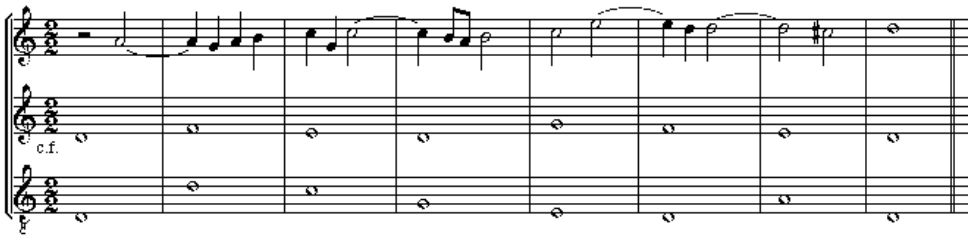
Beispiele: Von der ersten Art (siehe Notenbeispiel, es kommt eine Note im Kontrapunkt auf eine Note im Cantus Firmus: so heißt eine festgelegte Melodie, die von den anderen Stimmen umspielt wird, ohne selbst besonders weitgehend verändert zu werden)



über die dritte Art (es kommen vier Noten im Kontrapunkt auf eine Note im Cantus Firmus)



bis hin zur fünften Art (hier ist der Rhythmus im Kontrapunkt freier als in den anderen Arten)



zwei- bis vierstimmig; zum Anhören siehe etwa `https://www.youtube.com/watch?v=NOumWT4Z-LM`. Die Ausgabe ist eine PDF-Datei mit den Noten bzw. eine MIDI-Datei zum Anhören.

Die Komposition des Cantus Firmus und der ersten und zweiten Art (zweistimmig) ist schon komplett. Für dritte Art zweistimmig und erste Art dreistimmig existiert ein Common-Lisp-Programm. Ich werde viel Literatur in Form von Büchern und Weblinks mitbringen. Ich habe auch ein Programm, Counterpointer `http://www.ars-nova.com/cp/`, mit dem wir die Kompositionen auf Korrektheit überprüfen können.

Die Teilnehmer würden auf jeden Fall eine Menge über Programmieren mit C++14 im Team, Komponieren und Musiktheorie lernen.

Klassenstufe/Semester

egal

Voraussetzungen

grundlegende C++-Kenntnisse (müssen nicht so tief sein, man würde auf jeden Fall C++14 lernen), Noten und Intervalle lesen können

Kursleitung

Timo Keller

2 Typentheorie

Es gibt viele Möglichkeiten, die Mathematik zu formalisieren. Die üblichste von diesen Formalismen ist vermutlich Mengenlehre: Mathematische Objekte werden meistens als „Mengen mit zusätzlicher Struktur“ definiert. Die Mengenlehre ist allerdings in dieser Hinsicht nicht alternativlos und (bestimmte Arten von) Typentheorie(n) bieten hier eine andere gute Möglichkeit an.

In der Typentheorie gibt es (statt Mengen, die mit $\in$-Relation ineinander verschachtelt sind) Typen, deren „Bewohner“ durch gegebene Regeln (sog. *Konstruktoren*) „produziert“ werden können. Zum Beispiel kann ein Bewohner des Typs der natürlichen Zahlen als 0 oder Nachfolger einer anderen natürlichen Zahl konstruiert werden.

Insbesondere werden viele mathematische Konstruktionen (kartesische Produkte, Funktionsräume, ...), die in der Mengenlehre mit willkürlichen Wahlen verwirklicht werden, in der Typentheorie durch primitive Regeln gegeben. Dieses Phänomen ähnelt dem Praxis der vielen Gebiete der Mathematik, Objekte nicht mit expliziten Konstruktionen, sondern durch sog. universelle Eigenschaften zu beschreiben. Außerdem hat Typentheorie spannende Verbindungen mit vielen anderen Bereichen der Mathematik wie Homotopietheorie, konstruktive Mathematik und Kategorientheorie.

In diesem Kurs werden wir uns nach einem Crashkurs über formale Systeme mit verschiedenen Typentheorien beschäftigen und viele Aspekte der Mathematik darin neu entdecken. Gegen das Ende des Kurses könnten wir uns je nach Zeit, Interesse und Vorwissen in eins der folgenden Themen vertiefen:

- Beschreibung der Semantik durch (bestimmte Arten von) Kategorien,
- Homotopietheorie mit Räumen als primitive Objekte (statt „Mengen mit einer Topologie“),
- funktionale bzw. abhängig getypte Programmiersprachen.

Voraussetzungen

Für den Hauptteil des Kurses wird kein konkretes Vorwissen benötigt, sondern nur eine gewisse „mathematische Reife“, um Beweise zu nachvollziehen, verschiedene Beweisformen (durch Widerspruch, Induktion ...) zu erkennen und die Formalisierung der Mathematik in einer Metatheorie sinnvoll zu finden. Daher ist dieser Kurs sowohl für Schüler*innen, die sich seit einiger Zeit mit Mathematik beschäftigen, als auch für Student*innen geeignet.

Für die vertiefenden Themen werden zwar eventuell Vorkenntnisse in verschiedenen Bereichen benötigt, aber diese werden vor der Akademie abgesprochen und die entsprechenden Inhalte nur dann behandelt, wenn alle sich in dem Bereich wohl fühlen.

Kursleitung

Aras Ergus

3 Homotopietheorie

In diesem Kurs wollen wir verstehen lernen, was es mit diesem ominösen Begriff Homotopie auf sich hat. Grob gesagt geht es darum, ob sich Dinge ineinander deformieren lassen, ohne sie zu zerreißen oder zu verkleben. Ein klassisches Beispiel ist die Teetasse, die sich zwar in einen Doughnut, nicht aber in eine Wasserflasche verformen lässt.

Aber wie soll man von zwei Sachen eigentlich entscheiden, ob sie bis auf Verformung gleich sind¿ Ein erster Ansatzpunkt wäre, die Anzahl der Löcher zu zählen, da sich diese bei Verformungen nicht ändert. Wie aber soll man die Anzahl der Löcher präzise bestimmen¿ Und gibt es womöglich verschiedene Arten von Löchern, z.B. das des Doughnuts im Vergleich zum Hohlraum in einer Flasche¿ Ein erster Schritt zur Beantwortung wird fur uns die sogenannte *Fundamentalgruppe* $\pi_1(X)$ sein. Im Wesentlichen besteht sie aus allen Möglichkeiten, ein elastisches Gummiband im Objekt X zu verlegen, wobei wir nicht zwischen ineinander deformierbaren Bändern unterscheiden wollen. Eine genaue Betrachtung zeigt dann, dass $\pi_1(\text{Flasche}) = \{0\}$ und $\pi_1(\text{Doughnut}) = \mathbb{Z}$.

Interessanterweise hat bereits $\pi_1(X)$ Anwendungen weit jenseits der Bestimmung von Formen: unter anderem beweisen wir den Fundamentalsatz der Algebra, laut dem jedes nichtkonstante komplexe Polynom eine komplexe Nullstelle hat, und befassen uns mit der Frage, ob beziehungsweise wie man ein Bild mit einem Faden so an n Nägeln aufhängen kann, dass es herunterfällt, sobald man einen beliebigen dieser Nägel aus der Wand zieht.

Später im Kurs werden wir auch auf die höheren Analoga, die Homotopiegruppen $\pi_2(X)$ (in X verlegte ‚Gummitücher'), $\pi_3(X)$ (‚Wackelpudding', laut Nicholas), ... zu sprechen kommen. Je nach Interesse und Vorwissen der Kursteilnehmer können wir zudem die Homologiegruppen $H_0(X)$, $H_1(X)$, $H_2(X)$, ... betrachten. Allgemein wird es viele Gelegenheiten zur Mitwirkung am Kurs geben, sei es durch Mitbestimmung der Themen oder Bearbeitung von Übungsaufgaben.

Voraussetzungen

Dieser Kurs richtet sich an ältere Schüler und Studenten. Es wird außer Interesse am Thema kein Vorwissen benötigt. Abhängig vom Vorwissen der Teilnehmer werden uns deshalb in den ersten Kurseinheiten mit den grundlegenden Begriffen der Gruppe und des topologischen Raumes auseinandersetzen.

Kursleitung

Daniel Harrer (ζX)

4 Einführung in die Galoistheorie

Wieso eine Lösungsformel für alle Polynome eine Utopie ist und was das mit Konstruktionen durch Zirkel und Lineal zu tun hat.

Sicherlich kennen die meisten noch aus der Schule die sogenannte „Mitternachtsformel“ $\frac{-b\pm\sqrt{b^2-4ac}}{2a}$, welches die Lösungen der quadratischen Gleichung $ax^2 + bx + c = 0$ angibt. Weniger bekannt sind die entsprechenden Lösungsformeln für algebraische Gleichungen dritten und vierten Grades. Lange Zeit hat man auch nach einer Lösungsformel für Gleichungen höheren Grades gesucht. Heute weiß man, dass diese Bemühungen vergebens waren, und dass es keine derartige Lösungsformel für Gleichungen vom Grad fünf oder höher geben kann, sofern man nur die Grundrechenarten sowie das Wurzelziehen zulässt.

Damit verwandt ist die Frage, welche regelmäßigen n-Ecke sich ausschließlich mit Zirkel und Lineal konstruieren lassen. Hier lautet das Ergebnis, dass dies genau dann möglich ist, wenn n ein Produkt aus verschiedenen Primzahlen der Form $2^{2^a} + 1$ sowie einer Zweierpotenz ist.

Auf dem ersten Blick haben diese beiden Probleme nur wenig miteinander gemeinsamen. Wir werden im Kurs aber sehen, dass sich sowohl das Lösen von Gleichungen als auch geometrische Konstruktionen mit Hilfe der Galoistheorie untersuchen lassen. Diese Galoistheorie (benannt nach dem Mathematiker Évariste Galois) wird einen wichtigen Platz in unserem Kurs einnehmen.

Am Anfang des Kurses werden wir uns aber erst einige algebraischen Grundbegriffe erarbeiten, um solche Probleme mathematisch modellieren zu können. Zum Beispiel werden wir Gruppen und Körper als algebraische Strukturen kennenlernen, welche das Rechnen mit Zahlen auf beliebige Objekte (z.B. Drehungen im Raum) verallgemeinern. Ebenso werden wir detailliert untersuchen, was „Konstruktion mit Zirkel und Lineal“ und „Lösungsformel für Gleichung“ eigentlich genau bedeutet. Von diesen Grundlagen ausgehend werden wir uns dann langsam zur Galoistheorie vorarbeiten und damit schließlich die oben genannten Resultate beweisen.

Voraussetzungen

Ihr solltet wissen, was Polynome (sowas wie ax^2+bx+c) und lineare Gleichungssysteme sind. Außerdem solltet ihr bereit sein, euch in abstraktere mathematische Konzepte hinein zu denken, was euch aber nicht abschrecken sollte. Wir haben genug Zeit das zu erklären, und der Kurs soll sich explizit an Schüler richten.

Kursleitung

Tamás Korodi und Christoph-Simon Senjak

5 Kryptographie und Kryptoanalyse

In unserem Kurs werden wir uns mit Methoden der Kryptologie aus Vergangenheit und Moderne befassen.

Wir wollen uns dazu zuerst die Anfänge des Geheimhaltens von Texten ansehen: Wie entstanden Steganographie und Kryptographie, was waren und sind die Anfänge und Grundsteine dieses Gebiets. Diese, aus heutiger Sicht vielleicht primitiv anmutenden, Prinzipien wollen wir dann weiter entwickeln und nebenbei die historische Entwicklung, das Katz-und-Maus-Spiel zwischen Kryptographen und -analytikern, nachvollziehen.

Wir werden verschiedene Konzepte der Kryptologie klassifizieren und jeweils dazugehörige Methoden erlernen, analysieren und bisweilen auch beispielhaft anwenden – also Texte verschlüsseln und zu entschlüsseln versuchen.

Zu den voraussichtlich behandelten Themen gehören Cäsar-Verschlüsselung, Vigenère-Verschlüsselung, Anfänge der maschinellen Verschlüsselung, Enigma und ihre Entschlüsselung, Steganographie (u.a. durch Sprachbarrieren), Public-Key-Verfahren, Symmetrische Verschlüsselung, AES, RSA, Quantenkryptoanalyse, Quantenkryptographie, und mehr.

Der Kursstoff wird sich wesentlich an Inhalten des Buches "Geheime Botschaften" von Simon Singh orientieren, natürlich ohne die dahinter versteckten oder dazu notwendigen mathematischen Konzepte aus den Augen zu verlieren.

Voraussetzungen

Der Kurs ist geeignet für Teilnehmer aller Alters- und Schulklassen und niedriger Semester, soweit noch nicht viel über Kryptologie bekannt ist.

Kursleitung

Manuel Gundlach