Zeitschrift: Pionier : Zeitschrift für die Übermittlungstruppen

Herausgeber: Eidg. Verband der Übermittlungstruppen; Vereinigung Schweiz. Feld-Telegraphen-Offiziere und -Unteroffiziere

Band: 44 (1971)

Heft: 10

Artikel: Vocoder

Autor: Mäder, R.

DOI: https://doi.org/10.5169/seals-562906

lisations par un réseau de transmission sûr. Devrait également être assurée la permanence de l'exploitation au profit de l'administration militaire et fédérale, de l'instruction de la troupe et du service de la troupe elle-même;
- par l'attribution à tous les états-majors supérieurs d'ordinateurs mobiles, aptes au service en campagne;
- par des contrats à longue échéance avec des centres de calcul privés adéquats pouvant être entièrement militarisés en temps de guerre. Ces centres devraient être protégés, pour autant que possible. L'armée devrait s'occuper des systèmes de liaisons et des terminaux.

Il n'est pas possible, aujourd'hui, de définir laquelle des trois solutions est la meilleure; toutefois on peut penser que la première est celle qui présente le plus d'avantages.

En tout cas il est certain qu'il est nécessaire d'agir aujourd'hui avec décision, en faisant abstraction du perfectionnisme helvétique habituel. Il importe de donner a l'administration et aux états-majors supérieurs de l'armée un moyen dont l'utilité et la nécessité ne sont plus à démontrer.

La machine et les systèmes d'exploitation existants actuellement sur le marché civil, ainsi que les développements auxquels on peut s'attendre dans les prochaines années, en particulier dans le domaine des possibilités d'entrées de sorties graphiques, simplifieront considérablement le problème de la communication homme–machine et seront susceptibles de satisfaire aux besoins militaires.

L'utilisation par les états-majors militaires d'un futur système de traitement de l'information sera particulièrement marquée par:
- le principe d'une philosophie de mémoire unifiée pour le personnel, les moyens, les processus et l'environnement, permettant la création d'une banque d'information coordonnée, base d'un système de traitement de l'information très développé;
- un système de renseignements comprenant un ensemble automatique de présentation des positions de nos troupes et de l'adversaire, des informations de l'environnement, des informations des pertes et des dégâts, d'un sous-système pour les informations techniques des troupes du génie et de transmission;
- un système spécifique pour l'information concernant le personnel;
- un système logistique;
- un système pour le domaine des opérations;
- un système pour l'enseignement.

Je suis convaincu que le traitement électronique des informations contribuera grandement à l'amélioration de nos moyens de défense et de notre préparation militaire, ainsi qu'à la puissance de combat de notre armée. Aussi je voudrais vous demander, en tant qu'officiers d'une troupe de commandement, de vous employer en faveur de l'introduction de ces nouveaux moyens.

Aujourd'hui, comme il y a 8 ans, il s'agit dans le domaine de la conduite électronique de la guerre, de convaincre les adversaires et de donner à ces nouveaux moyens le rang qu'ils méritent.

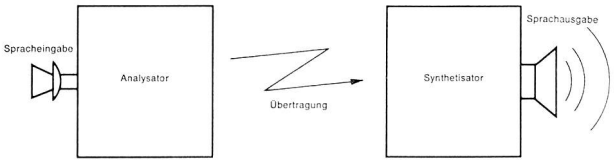
Bei den nachstehenden Aufsätzen handelt es sich um die Referate, die am Jahresrapport der Offiziere der Uebermittlungstruppen gehalten wurden. Sie zeigen, auf welchen Gebieten die elektronische Datenverarbeitung in der Armee bereits Anwendung findet. Red.

Vocoder

Die Sprache wird durch Luftschwingungen übertragen. Bell ist es gelungen, diese Luftschwingungen in elektrische Schwingungen umzuwandeln und umgekehrt. Damit war das Telephon erfunden. Der Vocoder ist eine andere Methode der Sprachübertragung. Um sie zu verstehen, müssen wir zuerst unsere Sprache genauer untersuchen.

Phonetiker haben herausgefunden, dass es nur etwa 50 verschiedene Lautwerte, sogenannte Phoneme, gibt. Wir produzieren etwa 10 Phoneme pro Sekunde. Formeln aus der Informationstheorie sagen uns, dass wir für die Sprachübertragung mit Phonemkette nur etwa 50 Bits pro Sekunde brauchen. Versucht man demgegenüber das Analogsignal der Sprache, wie es zum Beispiel über einen Telephondraht übermittelt wird, in Zahlenform darzustellen, so braucht man für eine gute Qualität etwa 64 000 Bits pro Sekunde. Also einerseits Phonemkette – theoretisch bloss 50 Bits, anderseits Analogsignal – 64 000 Bits pro Sekunde. Warum der Unterschied? Im Analogsignal ist einerseits mehr Information, anderseits mehr Redundanz. An Information habe ich zum Beispiel das Geschlecht des Sprechers, seine Stimmlage, seine Fehler und Versprecher sowie viele Nebengeräusche. Zudem habe ich eine Menge Redundanz, die in der Natur nötig ist, um eine gute Verständlichkeit auch in gestörter Umgebung zu gewährleisten. Die konventionelle Sprachübertragung mit einem Analogsignal bietet also viel mehr Möglichkeiten, als ich eigentlich ausnützen kann. Jeder normale Mensch hat nur eine Zunge und kann mit ihr nur sovielmal pro Sekunde wackeln. Ich kann ja beim Sprechen weder Trompete blasen noch Schlagzeug spielen, alles Tonspektren, die ich mit einem Analogsignal übertragen könnte. Aus diesen Überlegungen heraus hat man versucht, eine Sprechmaschine zu bauen, die in ihrer Funktion dem menschlichen Sprachorgan nachgebildet ist. Statt dass ich dann die Sprache selber übertrage, muss ich nur noch die Steuerimpulse übermitteln. Dazu brauche ich ein Gerät, welches aus der gesprochenen Sprache Steuerimpulse erzeugt. Analysator, Steuerbefehlsübertragung, Sprechmaschine, – das ist der Grundgedanke des Vocoders.

Vocoder Elemente

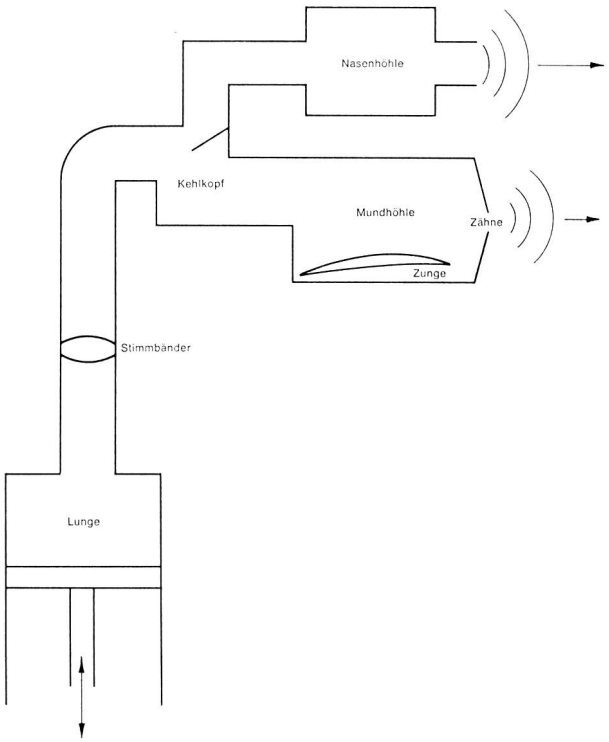


Vocoder ist die Abkürzung für Voice Coder. Eigentlich besteht ein Vocoder aus zwei Elementen: einem Voder und einem Coder. Der Coder oder Analysator wandelt die Sprachelemente in Codes um, der Voder oder Synthetisator tut das Gegenteil. Beginnen wir bei der Ausgabe, das heisst bei der Sprachnachbildung oder beim «Voder-Teil» des Vocoders. Zur künstlichen Spracherzeugung brauchen wir elektrische Schaltkreise.

Das Problem ist, sie richtig anzusteuern, und darin unterscheiden sich die verschiedenen Arten von Vocodern, auf die wir hier nicht einzeln eingehen können.

Wenden wir uns nach der Sprachsynthese dem Gebiet der Sprachanalyse zu.

Auf einem Oszillogramm zeigen selbst einfache Vokale wie AAAAAA, EEEEEE eine komplizierte Struktur. Noch ärger sehen Frikativlaute aus: SSSSSS, SCHSCHSCHSCHSCH-SCH, FFFFFF. Das Problem der Sprachanalyse ist, in diesen

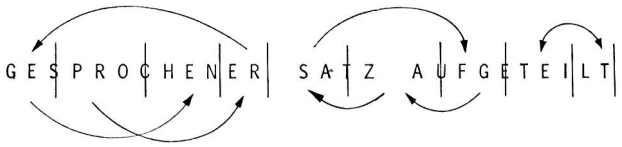


kann man die mit Pulse-Code-Modulation benötigte Bandbreite um einen Faktor 2 reduzieren, mit etwas mehr Aufwand um Faktor 4. Wird die Einschränkung akzeptiert, dass ausser Sprache nichts anderes übertragen werden soll, so kann man mit einer Bandbreite von 10K Bits schon fast einen HIFI-Vocoder bauen.

Das Thema des Jahresrapports lautete: Die Armee – die Uebermittlungstruppen – der Computer. Was haben Computer mit Vocoder zu tun?

Wie Sie vorher gesehen haben, ist die Sprachanalyse äusserst komplex. Computer können hiebei eingesetzt werden. Dank ihrer hohen Entscheidungstätigkeit kann dabei die Bit-Rate der Übertragung nochmals wesentlich gesenkt werden, bei gleichbleibender Qualität. Durch sogenanntes Pattern Matching wurde ein Vocoder konstruiert, der für die Übertragung von Sprache nur noch 960 Bits/sec braucht.

Zeitliche Verwürfelung

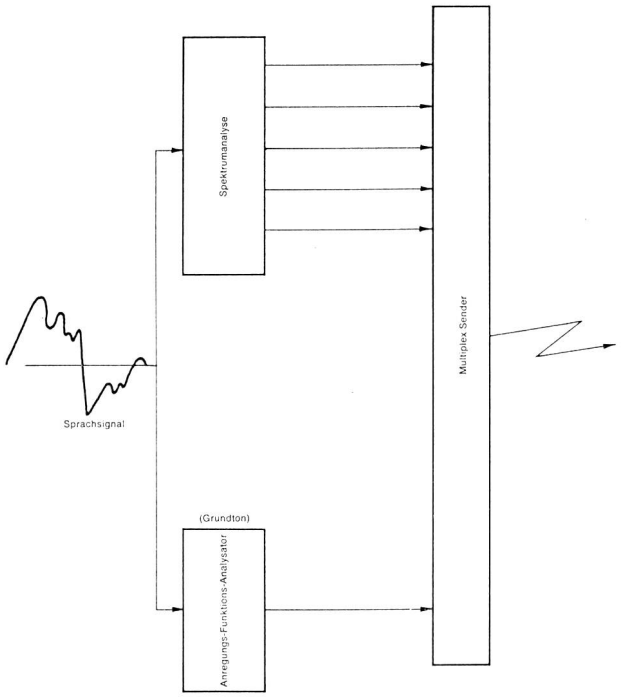


Schwingungen Grundton und Formanten zu lokalisieren, denn dies sind die wesentlichen Lautelemente, die es zu rekonstruieren gilt.

Die Aufgabe des Analysators ist es, diese Lautelemente zu erkennen und zu codieren. Neben dem Grundton werden auch einzelne Frequenzbänder gemessen.

Der Grundbau ist wichtig. Mit ihm allein kann man bereits den Rhythmus eines Satzes erahnen. Wenn der Grundbau durch Computer frisiert wird, erkennt man bereits etwa die Kadenz eines Fragesatzes. Zu diesem Grundton wird nun die übrige Sprachinformation hinzugemischt, und als Resultat bekomme ich einen verständlichen Satz.

Was hat nun ein solcher Vocoder, der übrigens schon 1939 von Dudley erfunden wurde, zu bieten? Ohne grosse Hexerei



Analysator

Lassen Sie mich nun einige Beispiele der Vocoder-Anwendung zitieren. Vocoder können Sprache nicht nur übertragen, sie können sie auch verbessern. Wenn Sie zwei Taucher unter Wasser hören würden, könnten Sie sich schon glücklich schätzen, überhaupt erkennen zu können, welche Sprache sie sprechen. Infolge der doppelt so hohen Schallgeschwindigkeit im Helium/Sauerstoff-Gemisch werden nämlich die Sprachlaute verzerrt; man spricht in diesem Zusammenhang von einem Donald-Duck-Effekt. Man kann diese Veränderungen in Spektrogrammen deutlich sehen. Da die Veränderungen bekannt sind, können sie auch rückgängig gemacht werden. Ein im IBM-Forschungslabor La Gaude entwickelter Vocoder überträgt die Sprache von Tauchern und korrigiert sie gleichzeitig.

Welches sind die militärischen Aspekte des Vocoders? Methoden der Sprachchiffrierung, die das analoge Sprachsignal verändern, wurden im letzten Weltkrieg eingesetzt. Durch Manipulationen, wie Inversion, Frequenzverschiebung, Time Division Scramblers usw., wurde versucht, das Sprachsignal unverständlich zu machen. Die ersten derartigen Systeme wurden von Amateurfunkern geknackt, und selbst das geheimste Übertragungssystem, über das sich Churchill und Roosevelt am Telephon unterhielten, wurde von den Deutschen mit Erfolg abgehorcht. Die Schwierigkeiten der guten Sprachchiffrierung liegen bei der grossen Redundanz der Sprache.

Die heutigen Systeme verwenden deshalb nicht mehr Analogsignale, sondern chiffrieren die digitalen Werte, die zum Beispiel aus Pulse-Code-Modulation gewonnen werden. Wendet man jedoch dabei das Einmalsystem nach Fried-

Pulse Code Modulation	ca. 50 000– 〉 100 000 Bits/Sek.
Vocoder	ca. 3 000–12 000 Bits/Sek.
Vocoder mit Computer	〈 1 000–ca. 3 000 Bits/Sek.

Das neue Kleinfunkgerät SE 19 von Autophon löst Kommunikationsprobleme

Bei öffentlichen Diensten, bei Bahnen, auf Baustellen, im Transportgewerbe, kurz: überall, wo schnelle und zuverlässige Verbindungen von Mensch zu Mensch notwendig sind, werden heute Kleinfunkgeräte eingesetzt.
Das neue, volltransistorisierte, tragbare Kleinfunkgerät SE19 von Autophon ist eine Weiterentwicklung der bekannten und erfolgreichen Serie SE 18. Wir haben es verbessert: es wurde noch kleiner, leichter und robuster. Trotzdem ist es ebenso vielseitig verwendbar und zuverlässig wie sein Vorgänger. Es arbeitet im 4-m-, 2-m- oder 70-cm-Band. Bei jedem Wetter, bei Hitze und Kälte.
Der Energiebedarf des SE 19 ist gering. Das ermöglicht eine lange Einsatzdauer. Die Stromversorgung lässt sich dem Verwendungszweck anpassen. Es wurde nach dem Baukastenprinzip konstruiert. Deshalb können Gerätevarianten für die verschiedensten Anforderungen geliefert werden.

Für Beratung, Projekte, Installation und Unterhalt **AUTOPHON**

Autophon kennt sich aus in Telephon- und Direktsprechanlagen, Personenruf- und Suchanlagen, Lichtruf, Signal- und Datenanzeigeeinrichtungen, elektrische Uhren und Rohrpost. Autophon-Sprechfunk in Fahrzeugen, tragbare Kleinfunkgeräte, drahtlose Telephonleitungen, Betriebsfernsehen, Musik zur Arbeit, Telephonrundspruch für Hotel und Spital.

Autophon AG

8059 Zürich	Lessingstrasse 1–3	051 27 44 55
9001 St. Gallen	Teufenerstrasse 11	071 23 35 33
4000 Basel	Schneidergasse 24	061 25 97 39
3000 Bern	Belpstrasse 14	031 25 44 44
2500 Biel	Plänkestrasse 16	032 2 83 62
6005 Luzern	Unterlachenstrasse 5	041 44 84 55
7000 Chur	Poststrasse 43	081 22 16 14
6962 Lugano	Via Bottogno 2	091 51 37 51

Téléphonie SA

1006 Lausanne	9, Chemin des Délices	021 26 93 93
1951 Sion	54, rue de Lausanne	027 2 57 57
1227 Genf	25, route des Acacias	022 42 43 50

Fabrikation, Entwicklungsabteilung und Laboratorien in Solothurn

75 Jahre
marktorientiertes Unternehmertum

Chr. Gfeller AG, 3018 Bern

mann an, so braucht man, um eine Minute sprechen zu können, etwa eine Million Chiffrierimpulse und hat zudem Probleme mit der Synchronisation.
Ein Vocoder braucht weniger Impulse zur Sprachübertragung, da er ja nicht die Sprache, sondern nur die Steuerimpulse überträgt; also kann man auch mit kleinerem Aufwand chiffrieren, und zudem ist die Redundanz weggelassen. Computer kann man hier dafür einsetzen, die Kombination Vocoder/Chiffriersystem zu simulieren, um die Wirksamkeit zu testen.

Pi Motf R. Mäder

Kryptoanalyse

Die Kryptoanalyse befasst sich mit der Aufgabe der Dekryptierung, das heisst mit dem Aufbrechen von aufgefangenen Chiffraten ohne Kenntnis der verwendeten Schlüssel. Im folgenden sei ein Beispiel für den Einsatz von Computern für derartige kryptoanalytische Aufgaben gegeben.
Wir gehen aus von einem konkreten handelsüblichen konventionellen Chiffriergerät. Ein solches präsentiert sich in folgender Form:

Ein Gerät mit
- einer Einrichtung für die Einstellung des Schlüssels (6 zweistellige Zahlen);
- einer Eingabemöglichkeit des zu chiffrierenden oder zu dechiffrierenden Textes (Tastatur);
- einer Schreib- oder Lesevorrichtung für den zugehörigen Chiffre- oder Klartext (Schreibstreifen).

Dieses Gerät führt im Innern Operationen aus (Ersetzen von Buchstaben nach einem arithmetischen oder Booleschen Formalismus), welche auch von einem Computer ausgeführt werden können. Es ist also durchaus möglich, einen Computer so zu progammieren, dass er dieses Chiffriergerät vollwertig simuliert oder sogar ersetzt.

Das notwendige zugehörige Programm umfasst
- das eigentliche Chiffrierprogramm, welches die inneren Funktionen des Chiffriergerätes enthält;
- die Eingabe des zu wählenden Schlüssels;
- die Eingabe des zu chiffrierenden Textes.

Über diese Verwendung als Chiffrierprogramm hinaus stellen wir nun die folgende kryptoanalytische Aufgabe:
Es sei ein Chiffrat aufgefangen worden, von dem wir wissen, dass es mit diesem Gerät hergestellt wurde, der dafür gewählte Schlüssel aber sei uns unbekannt. Bei bekanntem Schlüssel wären Chiffriergerät und Computer, abgesehen von der verschiedenen Arbeitsgeschwindigkeit, gleichwertig für die Dechiffrierung. Da wir aber in unserer Aufgabe den verwendeten Schlüssel zuerst suchen müssen, bietet uns der Computer dank seiner grossen Geschwindigkeit die naheliegende Möglichkeit, sämtliche Schlüssel des Gerätes systematisch abzusuchen.
Den Auftrag dazu geben wir dem Computer mit einem übergeordneten Such- oder Dekryptierprogramm mit folgendem Arbeitszyklus:

- Stelle einen ersten Schlüssel ein.
- Dechiffriere damit das aufgefangene Chiffrat.
- Prüfe auf Klartext, das heisst das Auftreten eines verständlichen Sinnes der Meldung.
- Entscheide:
  wenn ja: drucke den Klartext heraus;
  wenn nein: stelle den nächsten Schlüssel ein,

womit der Zyklus wieder anfängt.

Machen wir eine Zeitbilanz: Das Gerät hat eine Mannigfaltigkeit von $2{,}75 \cdot 10^9$ möglichen Schlüsseln. Diese Zahl entspricht
- in msec gemessen 32^d
- in µsec gemessen 46^m

Bei der für einen der oben beschriebenen Arbeitszyklen benötigten Zeit (Grössenordnung msec) haben wir also mit einer Computerzeit von mehreren Tagen zu rechnen. Diese Dauer gibt uns übrigens einen Hinweis auf die Güte des gewählten Chiffriergerätes.
Das Absuchen können wir durch folgende Ergänzung beschleunigen:
Wir nehmen an, in unserem aufgefangenen Text komme ein bestimmtes Klarwort vor (es ist dies die Methode des «mot probable» in der Kryptologie). Solche Annahmen sind bei militärischen Texten naheliegend, wir wählen für unseren Fall das meistverwendete Wort «Angriff».
Der Umstand, dass der Computer nun nicht mehr irgendeinen Klartext, sondern einen bestimmten Klartextausschnitt zu suchen hat, erlaubt im vorliegenden Chiffrierverfahren ein gezieltes Absuchen der möglichen Schlüssel, so dass wir statt der ursprünglichen $2{,}75 \cdot 10^9$ Fälle nur mehr deren 50 000 zu prüfen haben. Damit sind wir im Bereiche des hier Möglichen.
Wir geben nun dem Computer über das Terminal den Auftrag:

- Lies das aufgefangene Chiffrat.
- Lege das Klarwort «Angriff» an die erste Stelle desselben.
- Prüfe, ob einer der noch zugelassenen möglichen Schlüssel die Zuordnung Chiffrat–Klarwort erlaubt.
- Entscheide:
  wenn ja: dechiffriere das ganze Chiffrat und drucke den Text heraus;
  wenn nein: lege das Klarwort an die zweite Stelle,

und so fort.

Der Computer liefert uns die Antwort, bestehend aus 8 möglichen Texten, die alle das Klarwort «Angriff» enthalten. Einer dieser Texte scheint uns einen vernünftigen Inhalt zu liefern («allgemeine Lage: Rot der durch einen starken Angriff von Grün im Raume ...»), das wir als richtigen Klartext für unser aufgefangenes Chiffrat ansprechen dürfen. Die sieben anderen Texte scheiden wegen Unverständlichkeit aus.
Wir haben bei diesem Beispiel Glück gehabt, dass wir nur eine Auswahl von 8 Texten auf vernünftigen Sinn prüfen mussten. Was ist aber zu tun, wenn statt nur 8 deren 8000 oder noch mehr Texte zur Auswahl herausgedruckt würden, was bei einem stärkeren Chiffriergerät mit grösserer Schlüsselmannigfaltigkeit ohne weiteres zu erwarten wäre? Das Absuchen durch den Menschen auf vernünftigen Text ist dann hoffnungslos.
Wir helfen uns, indem wir dem Computer ein Klartextkriterium einbauen. Zwar ist der Computer nicht imstande, auftretende Dechiffrate intelligenzmässig zu verstehen; wir können ihn aber so programmieren, dass er auf bestimmte Klartextmerkmale achtet und sie zweckmässig bewertet. Im allgemeinen werden wir den Computer nur die höchstbewerteten Texte ausdrucken lassen. So haben wir dann nur noch wenige Fälle intelligenzmässig auf vernünftigen Sinn zu prüfen.
Im vorliegenden Beispiel liegt zwischen der Eingabe unseres Auftrages an den Computer und dem Herausdrucken seiner Antwort eine Rechenzeit von 65^m. Diese Rechenzeit ist hauptsächlich bedingt durch die Zugriffszeit des für diese Aufgabe benötigten externen Speichers; sie lässt sich bei moderneren Anlagen wesentlich verkürzen.
Diese Zeitspanne dient uns als Mass für die Sicherheit eines Chiffriergerätes. Nach heutiger Auffassung handelt es sich um ein konventionelles Chiffrierverfahren mittlerer Kapazität, die sich durch Verwendung weiterer Bauelemente um mehrere Zehnerpotenzen verbessern liesse. Damit ist gezeigt, dass der Wettlauf zwischen Chiffrierverfahren und Computer noch nicht entschieden ist.

Major P. Glur