# Toward combinatorial proof of P < NP

L. Gordeev

Tübingen-Utrecht

June 2006

# DNF-Validity (Val)

- DNF: Any expression Φ of the form

$$\sum_{i=1}^{n} \prod_{j=1}^{n} l_{i,j} \; for \; l_{i,j} \in \{x_k, \neg x_k\}$$

where $a+b := a \vee b, a \cdot b := a \wedge b$

- DNF Φ is *valid* iff BoolVal(Φ) = 1

for all BoolVar $x_k \in \{0,1\}$

# CNF-Satisfaction (Sat)

- CNF: A dual-DNF expression Φ

$$\prod_{i=1}^{n} \sum_{j=1}^{n} l_{i,j} \; for \; l_{i,j} \in \{x_k, \neg x_k\}$$

where $a + b := a \vee b, \; a \cdot b := a \wedge b$

- CNF Φ is *satisfied* iff BoolVal(Φ) = 1 for some BoolVar $x_k \in \{0,1\}$

# P vs. NP (P-NP) Problem

- Conjecture P = NP (S.A. Cook, 1971, a.k.a. Clay Millennium Problem #4) says that e.g.

  CNF-Sat problem:

  „***Is a given CNF*** $\Phi$ ***satisfied*** ?“

  is decidable by a Turing Machine in polynomial time (w.r.t. the length of $\Phi$)
- One can replace CNF-Sat by DNF-Val: „***Is a given DNF*** $\Phi$ ***valid*** ?“
- So far $P \neq NP$ appears more plausible

# Prophecy

Harvey Friedman, October 20, 2005:

*2050, $P \neq NP$. Detailed combinatorial work on easier problems, leading up to the full result. $P = PSPACE$ will be refuted first.*

# On algebraic interpretation 1

Consider boolean DNF upgrade of „school-algebraic“ conversion ***EXPAND*** distributing products over sums

Let $f := ((x + y)z + y(x + \bar{x}))(x + z)$

$\mathit{EXPAND}(f) =$

$x^2y + x^2z + xz^2 + yz^2 + 2xyz + yx\bar{x} + yz\bar{x} =$

$xy + xz + yz$

<u>Note</u>: $\mathit{EXPAND}(f)$ unique, if positive

# On algebraic interpretation 2

- **Known and easy:**

  ***EXPAND****(f) has no f-polysize upper bound*

- **Reverse problem:**

  *How large must be f such that positive*

  ***EXPAND****(f) is „large & complex“?*

- **Claim**: *Reverse problem is closely related to* $\boldsymbol{P \neq NP}$

# On algebraic interpretation 3

- Trouble: Positive polynomials are essential for uniqueness, but too restrictive in boolean domain
- Hint: There is no valid positive boolean DNF
- Generally: Boolean space is too primitive

  for genuine mathematical investigations
- Solution: Expand *discrete* Boolean space to boolean-valued Borel (abbr.: BBorel) space and use *analytic* methods

# BBorel polynomials

1. Literals: $x +_{\mathbb{R}} y = 0$ , $x +_{\mathbb{R}} y \neq 0$
2. Boolean operations: $a \vee b$, $a \wedge b$

   (usual abbr.: *a*+*b*, *ab*)
3. That is, BBorel polynomials are boolean polynomials w.r.t. Borel atoms $x +_{\mathbb{R}} y = 0$
4. Semantics: $x +_{\mathbb{R}} y$ refers to the addition of reals *x*, *y*

# How it works

- Boolean *n*-dim DNF family is represented by 1 „universal“ positive BBorel CNF $\Phi_n$
- <u>THEOREM</u>

  $Val \subset P/poly \Rightarrow \exists c \forall n( \exists n^c$-size BBorel $f$ )
  *(* $f \approx \Phi_n$ *and hence* ***EXPAND(f)=EXPAND(*** $\Phi_n$ ***))***
- Hence P $\neq$ NP holds, if $f$ as above fails
- <u>Note</u> „≈“ means semantical equivalence in Continuum!

# Shape of $\Phi_n$ and beyond

$$\Phi_n := \prod_{f:\boldsymbol{n}\to\boldsymbol{n}} \sum_{i<j\in\boldsymbol{n}} \left(x_{f(i),i} +_{\mathbb{R}} x_{f(j),j} = 0\right) \in \prod\nolimits_2^0 \text{ where}$$

$$\boldsymbol{n} = \{1,\cdots,n\}$$

$\boldsymbol{EXPAND}(\Phi_n) \in \sum_2^0$ is *„large & complex“*
*(of course exponential in n)*

*It remains to prove that* $\forall c\, \exists n$ *so large that*

*there is no* $n^c$*-size* $f \in \boldsymbol{EXPAND}^{-1}(\boldsymbol{EXPAND}(\Phi_n))$

*This admits plain combinatorial translation* CombState.pdf

# Combinatorial challenge

1. The desired proof is easy for $f \in \sum_2^0, \prod_2^0$
2. Extension to $f \in \sum_3^0, \prod_3^0$ :

   No new ideas – only precise asymptotical estimates on the number of clauses occurring in ***EXPAND****($\Phi_n$)* and appropriate partitions of sets of natural numbers

   ( pure combinatorics )

CombProblems.pdf

# General case $f \in \sum_k^0, \prod_k^0, k > 3$

- Presumably the same method in nested form
- Higher (bounded!) quantifier complexity of the auxiliary definitions
- More asymptotical combinatorics
- Just ordinary mathematical work
- If counterexample, then Local P=NP holds!

# Remarks

1. BBorel version of ***EXPAND*** slightly differs from „school-algebraic“ ***EXPAND***
2. $f \approx g \Rightarrow$ ***EXPAND(f)*** = ***EXPAND(g)*** is the crucial implication (semEq $\Rightarrow$ synEq) in both cases
3. The BBorel case is proved via geometry
4. BBorel polynomials *f*, *g* involved have familiar $\Sigma^0_k, \Pi^0_k$ structure; „*k*“ = natural proof parameter
5. Asymptotical combinatorics to be employed

# Nature: P = NP ?

Protein Folding Problem: **Given a stable protein as a long string over 20 amino acids identify its unique 3D structure with minimal energy**. This problem is NP-hard under all mathematical models. Hence no polynomial-time solution can be achieved by the known mathematical algorithms, and yet it takes at most a few seconds to obtain the result in reality.