Democracy as a Critical System:

Security, Formal Methods, and Elections

Joseph Kiniry
IT University of Copenhagen

applied
formal
methods

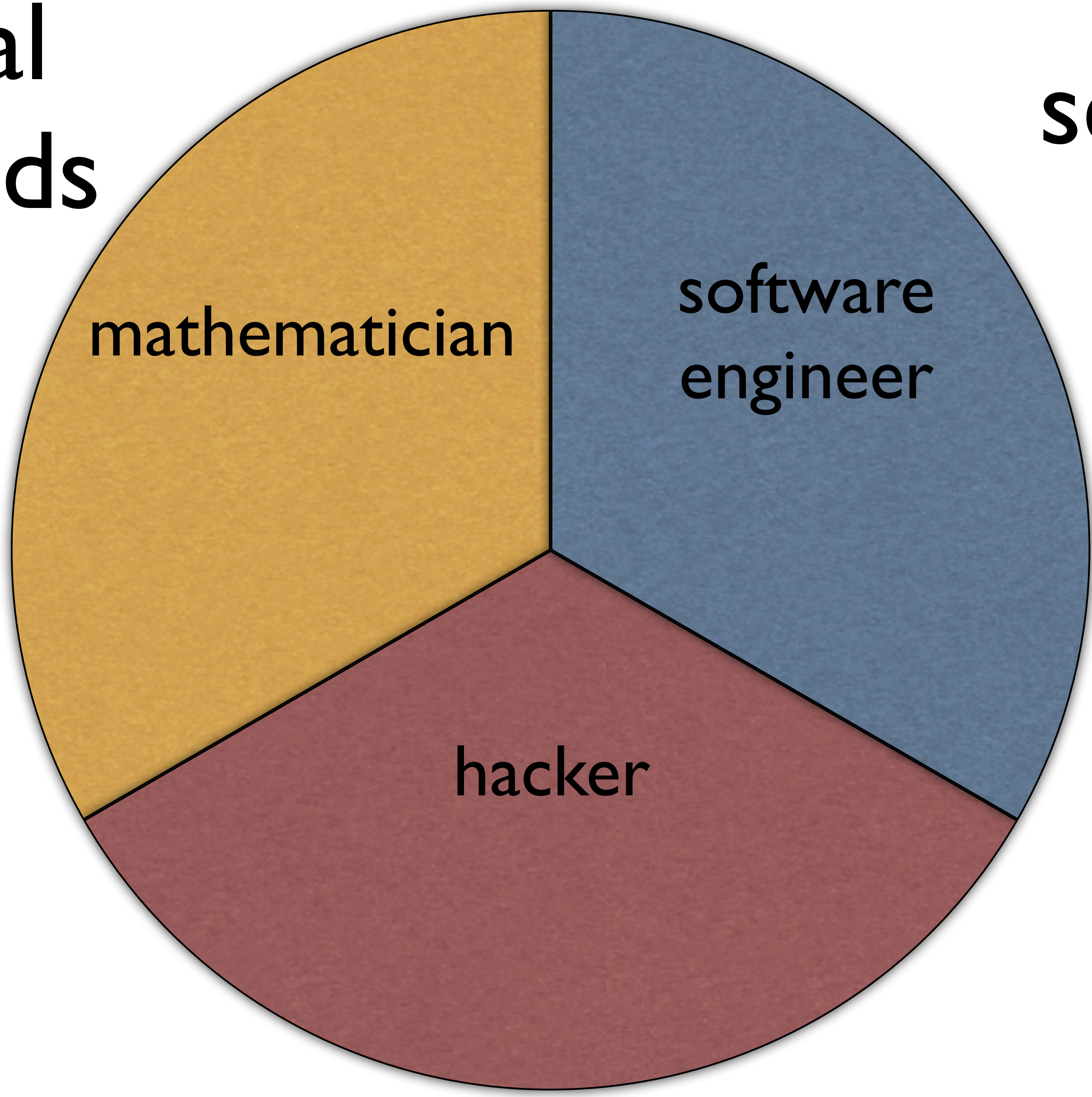
IT
security

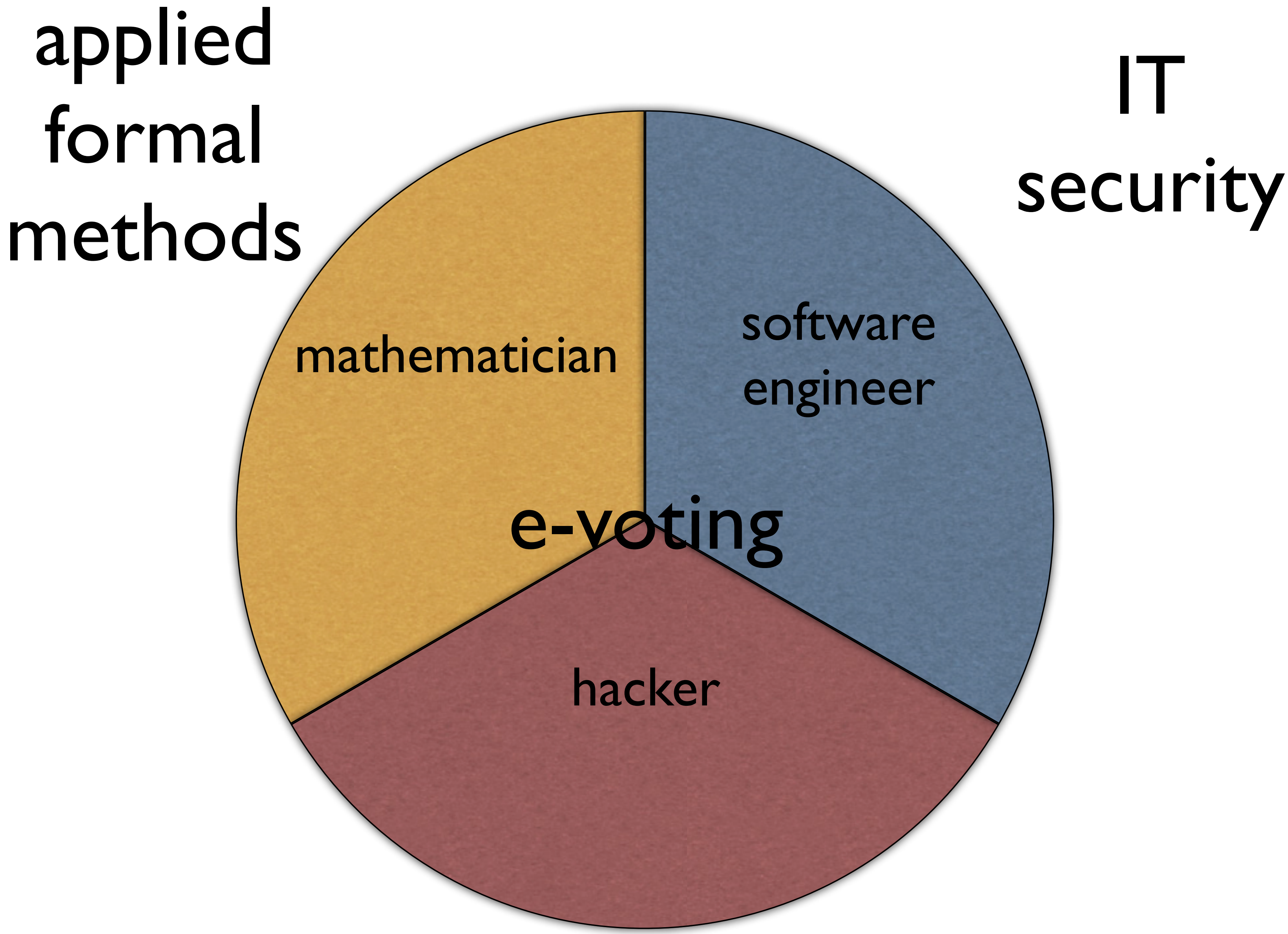
applied
formal
methods

IT
security

applied formal methods

IT security




applied
formal
methods
IT
security
mathematician
software
engineer
e-voting
hacker

military

biomedical

avionics

automotive

Critical Systems

financial

aeronautics

nuclear

transport

voter
registration

voter
trust

government
legitimacy

voting
systems

Democracy

voting
schemes

casting
ballots

election
outcomes

counting
ballots

society

troublemaker

impact

Activism and Science

good

education

obligation

punchcard
ballots

mechanical
ballot boxes

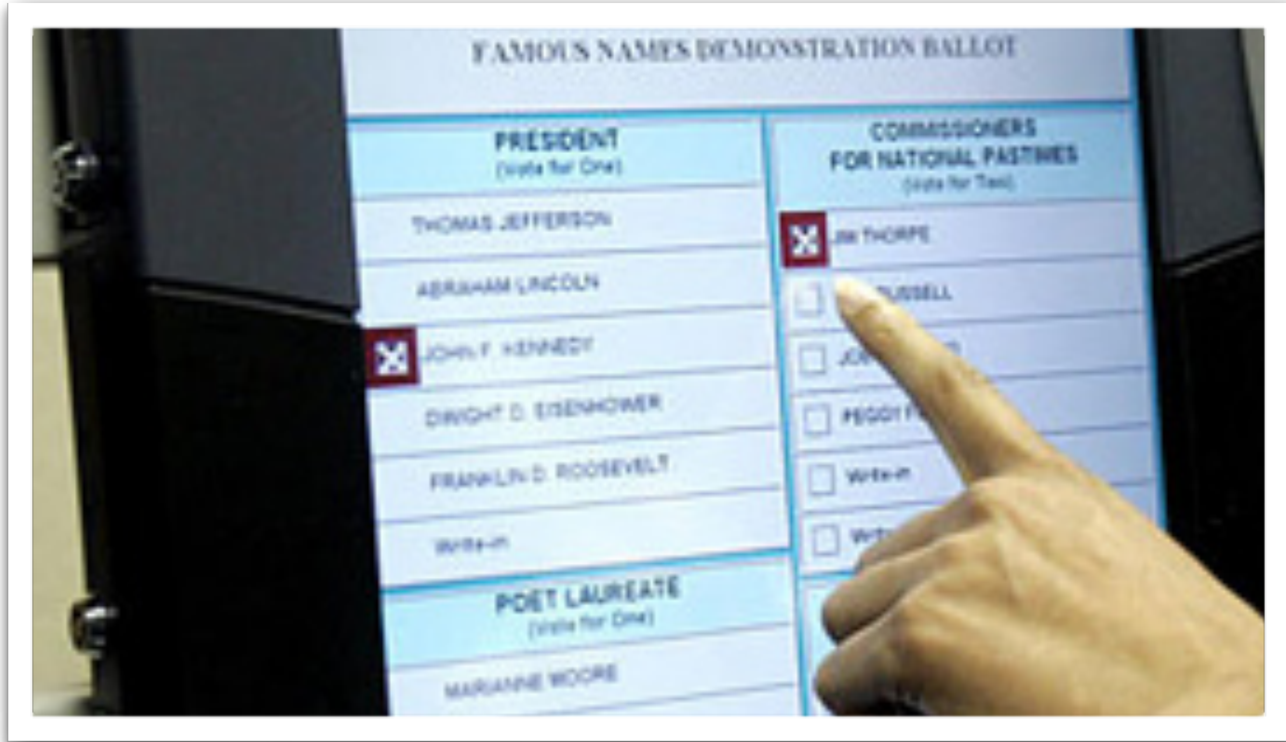
physical
locks

Voting Machines

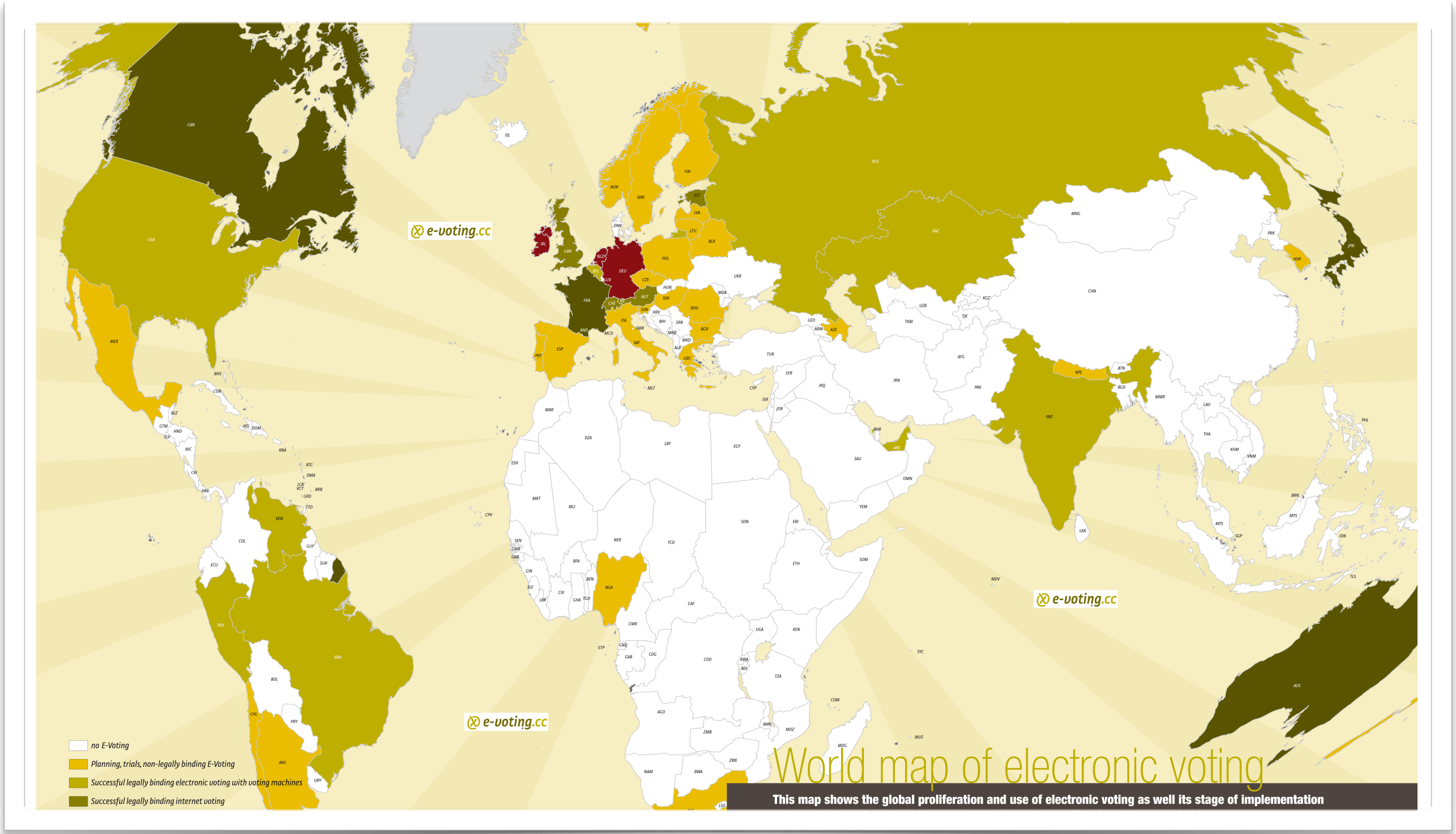
dedicated
primitive
hardware

lever
machines

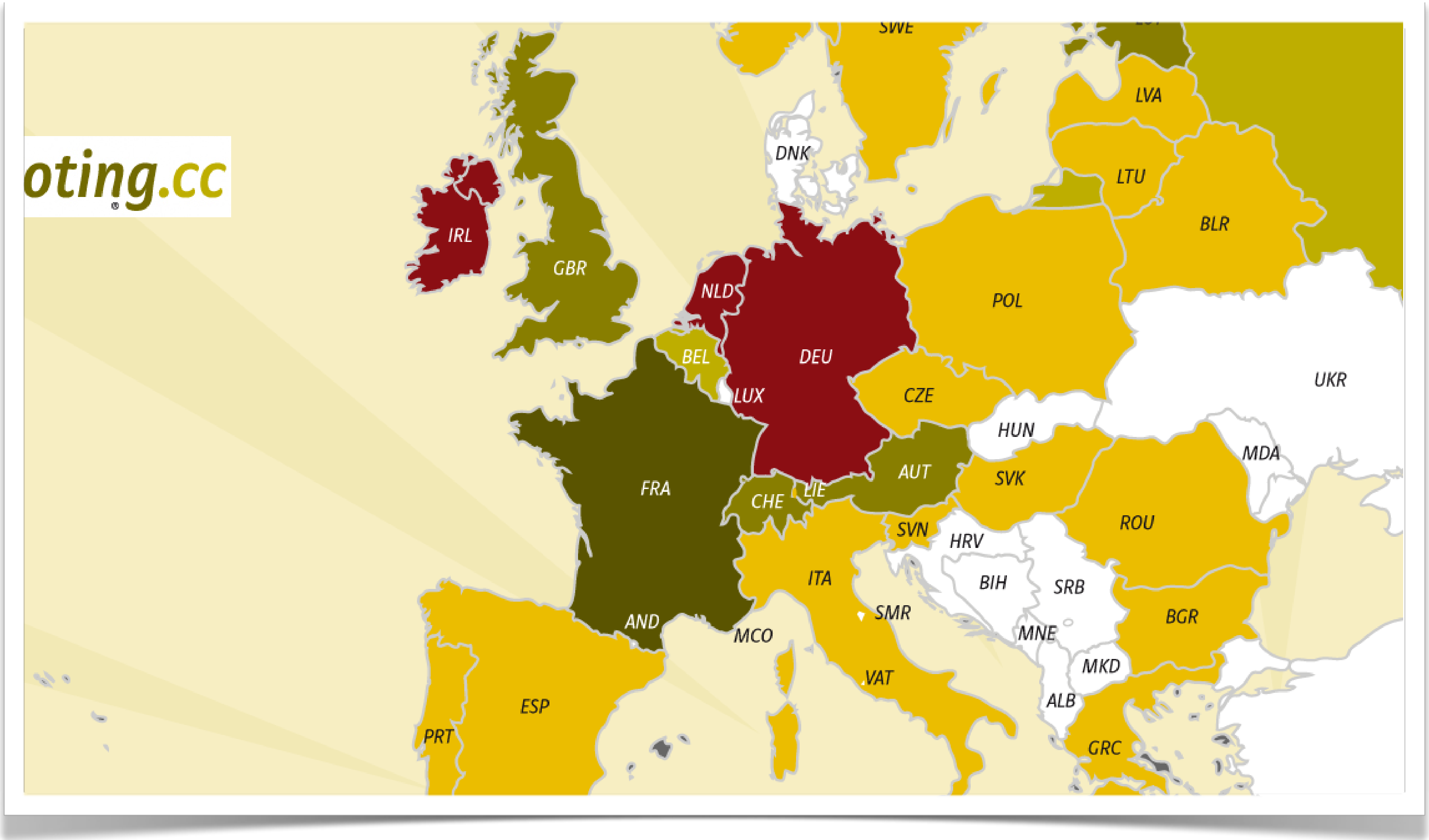
off-the-shelf
Windows
machines



e-Voting Worldwide



e-Voting Worldwide



e-Voting in the EU

dedicated computer-based voting machines since the late 90s

people generally trust the government

experiments in remote voting for expats

Computer-based Voting in The Netherlands

hacking an election

tally system developed with formal methods

recommendations to the government

KOA

PR-STV

novel social vote counting

last-minute secret purchase of €40M in Nedap machines

Computer-based Voting in Ireland

PowerVote

Vótáil

independent system testing

CEV

scrapping e-voting at a cost of €55M

people generally trust the government

claim: no computers are used in voting

in truth: closed-source tally system used to compute final outcome

Computer-based Voting in Denmark

regular proposals to introduce e-voting

DiVS

e-voting trials at the local level

DemTech

experiences with open source e-voting systems

experiences with proprietary e-voting systems

Experiences in Hacking Voting Systems

hacking remote elections

hacking kiosk-based voting computers

analyzing academic voting systems

most open source voting systems are not tested

most proprietary voting systems are not tested

Testing Voting Systems

"hard-core" testing is random testing of multiple implementations

random testing is no testing

how does one rigorously test a voting system?

Relating The Law to Software

The State of e-Voting Software Today

Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;

2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or

3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

1.2.3. Step Three: Allocating Compensatory Seats to Parties

This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

The Law

```
char*M,A,Z,E=40,J[40],T[40];main(C){for(*J=A=scanf(M="%d",&C);
--            E;             J[             E]             =T
[E   ]=  E)   printf("._");  for(;(A-=Z=!Z)  ||  (printf("\n|"
)    ,   A    =              39              ,C             --
)    ;   Z    ||    printf   (M   ))M[Z]=Z[A-(E   =A[J-Z])&&!C
&    A   ==             T[                                  A]
|6<<27<rand()||!C&!Z?J[T[E]=T[A]]=E,J[T[A]=A-Z]=A,"_.":" |"];}
```

e-Voting Software

$\emptyset$

Refinement Relation

In our tests, it counts correctly.

Overall Correctness Argument

Trust us, it works.

How hard can it be, adding one over and over?

The State of *Verified* e-Voting Software Today

concept analysis

Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;
2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or
3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

1.2.3. Step Three: Allocating Compensatory Seats to Parties

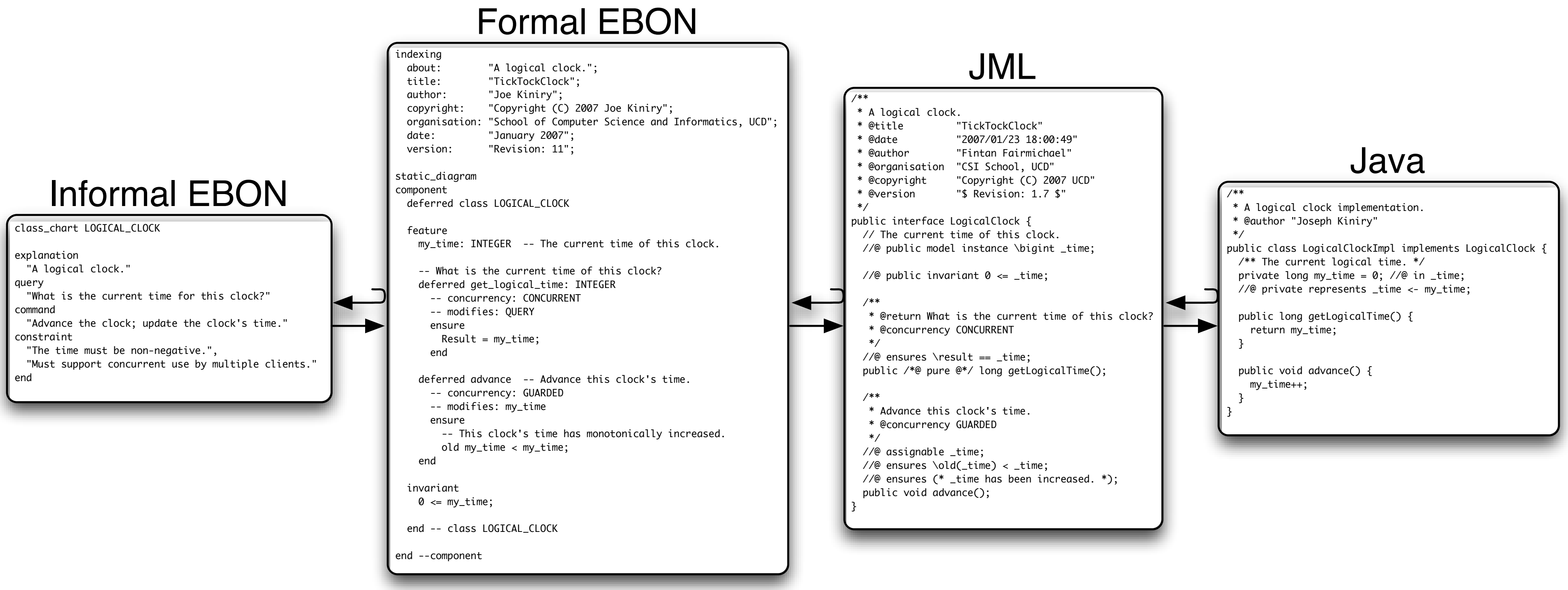
This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

invariants

The Law



e-Voting Software

Danish Law

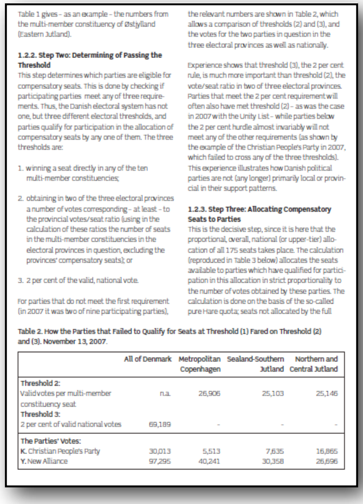


Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;
2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or
3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

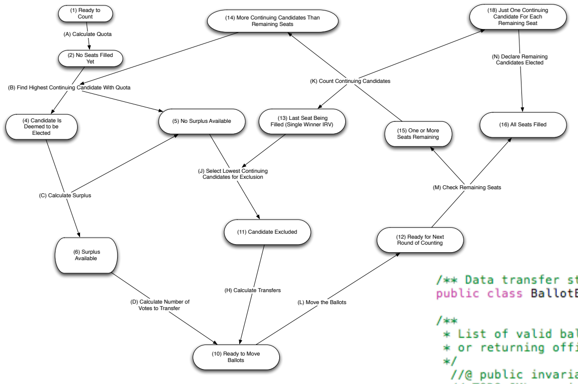
1.2.3. Step Three: Allocating Compensatory Seats to Parties

This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

Verified Software




```java
/** Data transfer structure for set of all valid ballots */
public class BallotBox {

/**
 * List of valid ballot papers, already shuffled and mixed by the data loader
 * or returning officer.
 */
  //@ public invariant \nonnullelements (ballots);
  // TODO JML warning: array nullity is invariant for assignment
  protected /*@ non_null spec_public @*/ Ballot[] ballots = new Ballot [Ballot.

    /**
     * Get the number of ballots in this box.
     *
     * @return the number of ballots in this ballot box
     */
   /*@ public normal_behavior
     @   ensures 0 <= \result;
     @   ensures \result == numberOfBallots;
     @   ensures (ballots == null) ==> \result == 0;
     @*/
    public /*@ pure @*/ int size(){
        return numberOfBallots;
    }

  /**
   * The total number of ballots in this ballot box.
   */
    /*@ public invariant 0 <= numberOfBallots;
      @ public invariant numberOfBallots <= Ballot.MAX_BALLOTS;
      @ public constraint \old (numberOfBallots) <= numberOfBallots;
      @*/
    protected /*@ spec_public @*/ int numberOfBallots;

    /**
     * Number of ballots copied from box
     */
    //@ public initially index == 0;
    //@ public invariant index <= size();
    //@ public constraint \old(index) <= index;
    protected /*@ spec_public @*/ int index;

    /**
     * Create an empty ballot box.
     */
    //@ assignable ballots, index, numberOfBallots;
    public /*@ pure @*/ BallotBox(){
```

Refinement Relation

If the input is as we characterized, then we guarantee a correct tally as output.

Overall Correctness Argument

Proof is aggregate modular verification of system's components.

Governments

do not trust

Verification

Governments
think they trust
Testing

Automated Testing
that complements
Formal Verification

Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;

2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or

3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

1.2.3. Step Three: Allocating Compensatory Seats to Parties

This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

The Law

Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;
2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or
3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

1.2.3. Step Three: Allocating Compensatory Seats to Parties

This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

```
-- An individual person standing for election
sig Candidate {
 votes:          set Ballot,   -- First preference ballots assigned to this candidate
   transfers: set Ballot,  -- Second and subsequent preferences received
   surplus:      set Ballot,    -- Ballots tranferred to another candidate election
 wasted:         set Ballot,  -- Ballots non-transferable due to exhaustion of preferences
   outcome:      Event          -- Election result for candidate and associated ballots
} {
   // Non-transferable ballots
   0 < #wasted implies (outcome = WinnerNonTransferable or
                   outcome = QuotaWinnerNonTransferable or
                   outcome = EarlyLoserNonTransferable or
                     outcome = SoreLoserNonTransferable)
   (outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
    implies wasted in surplus
   (outcome = EarlyLoserNonTransferable or outcome = SoreLoserNonTransferable)
    implies wasted in votes + transfers
   // Division of ballots into first preferences and transfers
     no b: Ballot | b in votes & transfers
   // Division of ballots into piles for each candidate
     all b: Ballot | b in votes + transfers implies this in b.assignees
   // Selection of surplus ballots for re-distribution
     surplus in votes + transfers
     Election.method = Plurality implies #surplus = 0 and #transfers = 0
     0 < #transfers implies Election.method = STV
   // Calculation of surplus for PR-STV election
   ((outcome = Winner and Election.method = STV) or (
    outcome = SurplusWinner or outcome = WinnerNonTransferable)) implies
    Scenario.quota + #surplus = #votes
     (outcome = Winner or outcome = SurplusWinner or
    outcome = WinnerNonTransferable) implies #transfers = 0
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies surplus in transfers
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies
         Scenario.quota + #surplus = #votes + #transfers
     0 < #surplus implies (outcome = SurplusWinner or outcome = AboveQuotaWinner or
                 outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
     (outcome = EarlyLoser or outcome = TiedEarlyLoser or
    outcome = EarlyLoserNonTransferable) iff
        (this in Scenario.eliminated and
    not (#votes + #transfers < Scenario.threshold))
     // All non-sore losers are at or above the threshold
   outcome = TiedLoser implies Scenario.threshold <= #votes + #transfers
```

e-Voting Test Harness

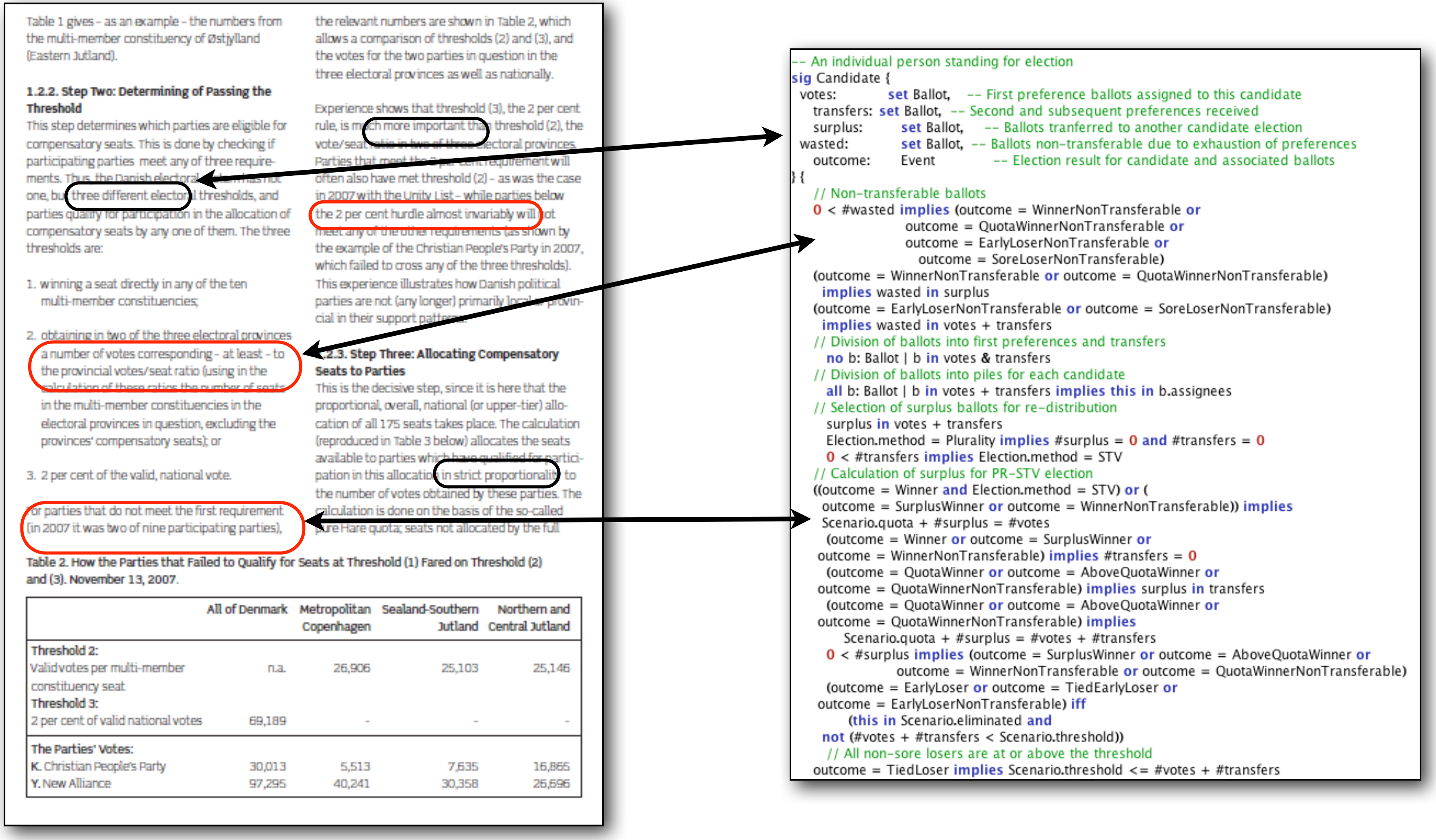


Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;
2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or
3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

1.2.3. Step Three: Allocating Compensatory Seats to Parties

This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

```
-- An individual person standing for election
sig Candidate {
 votes:          set Ballot,   -- First preference ballots assigned to this candidate
   transfers: set Ballot,  -- Second and subsequent preferences received
   surplus:        set Ballot,    -- Ballots tranferred to another candidate election
 wasted:            set Ballot,  -- Ballots non-transferable due to exhaustion of preferences
   outcome:        Event           -- Election result for candidate and associated ballots
} {
   // Non-transferable ballots
   0 < #wasted implies (outcome = WinnerNonTransferable or
                     outcome = QuotaWinnerNonTransferable or
                     outcome = EarlyLoserNonTransferable or
                       outcome = SoreLoserNonTransferable)
   (outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
     implies wasted in surplus
   (outcome = EarlyLoserNonTransferable or outcome = SoreLoserNonTransferable)
     implies wasted in votes + transfers
   // Division of ballots into first preferences and transfers
     no b: Ballot | b in votes & transfers
   // Division of ballots into piles for each candidate
     all b: Ballot | b in votes + transfers implies this in b.assignees
   // Selection of surplus ballots for re-distribution
     surplus in votes + transfers
     Election.method = Plurality implies #surplus = 0 and #transfers = 0
     0 < #transfers implies Election.method = STV
   // Calculation of surplus for PR-STV election
   ((outcome = Winner and Election.method = STV) or (
     outcome = SurplusWinner or outcome = WinnerNonTransferable)) implies
     Scenario.quota + #surplus = #votes
     (outcome = Winner or outcome = SurplusWinner or
    outcome = WinnerNonTransferable) implies #transfers = 0
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies surplus in transfers
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies
        Scenario.quota + #surplus = #votes + #transfers
     0 < #surplus implies (outcome = SurplusWinner or outcome = AboveQuotaWinner or
                       outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
     (outcome = EarlyLoser or outcome = TiedEarlyLoser or
    outcome = EarlyLoserNonTransferable) iff
          (this in Scenario.eliminated and
    not (#votes + #transfers < Scenario.threshold))
     // All non-sore losers are at or above the threshold
   outcome = TiedLoser implies Scenario.threshold <= #votes + #transfers
```

e-Voting Test Harness

Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;

2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or

3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

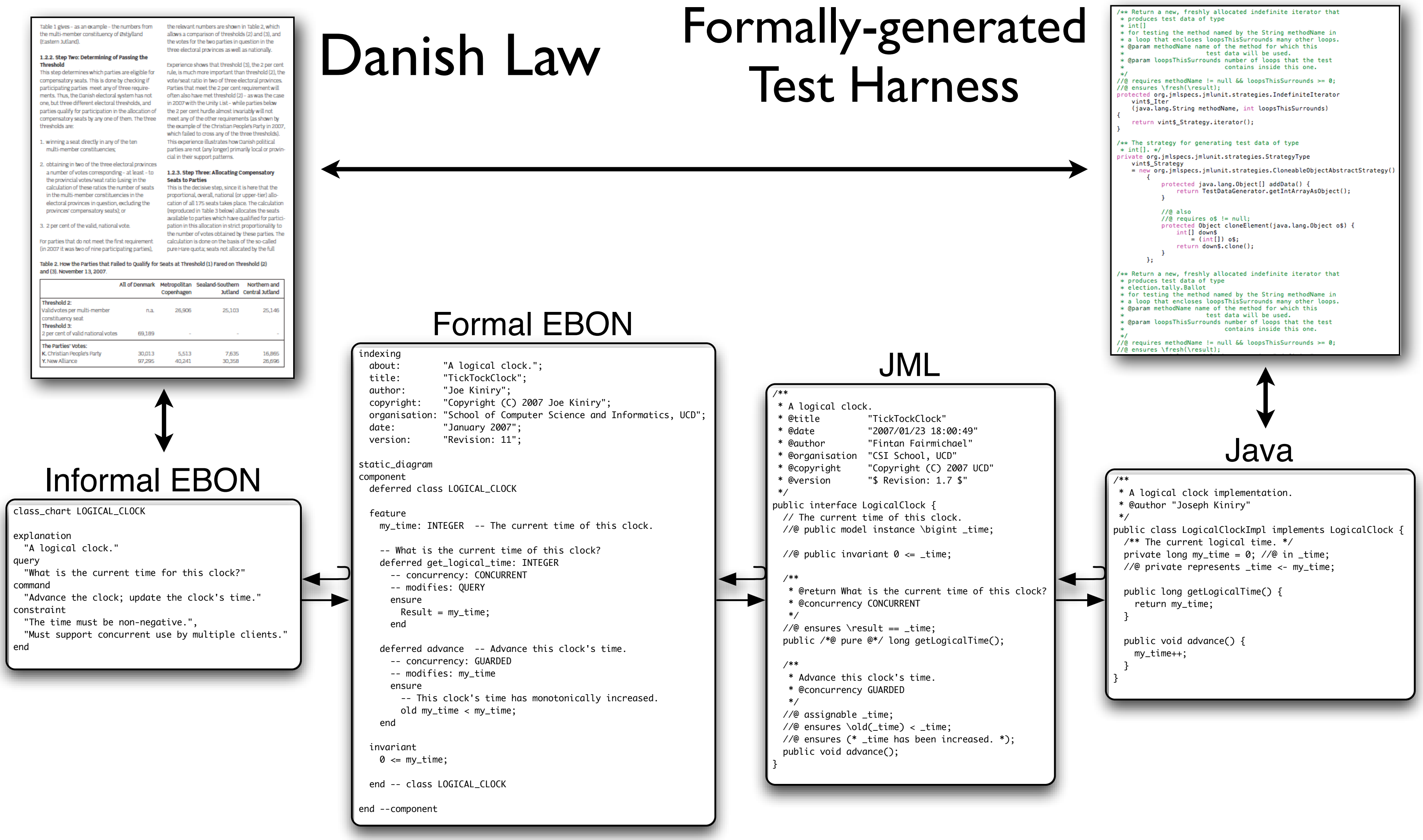
1.2.3. Step Three: Allocating Compensatory Seats to Parties

This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

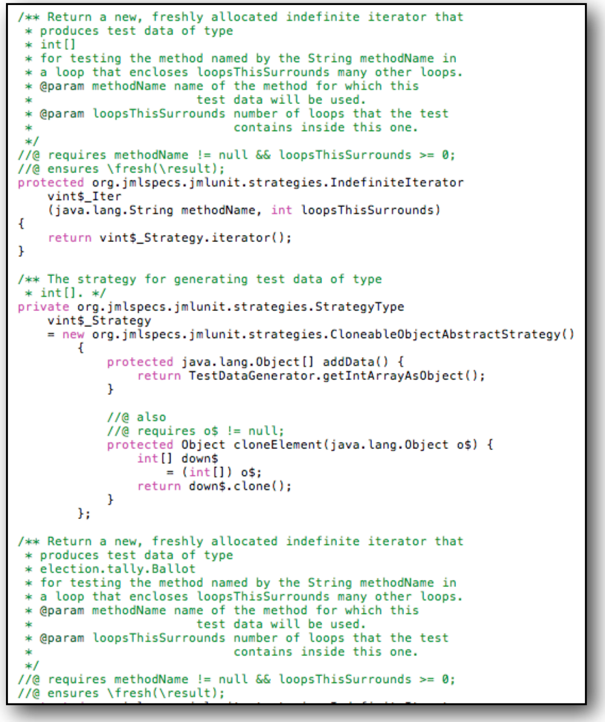
	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

e-Voting Test Harness



Refinement Relation

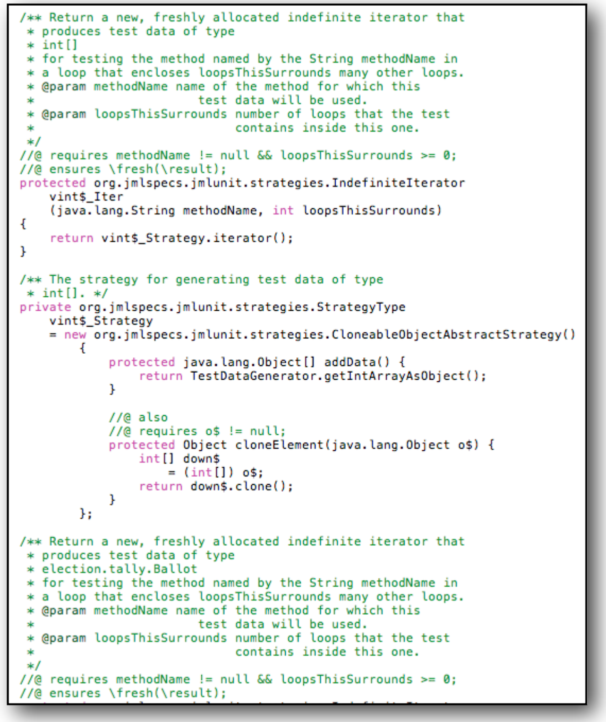
```java
public class Ballot {
    private static final char WHITE_SPACE = ' ';

    /**
     * Maximum possible number of ballots based on maximum population size for a
     * five seat constituency i.e. at most 30,000 people per elected
     * representative.
     *
     * @see "Constitution of Ireland, Article 16, Section 2"
     */
    public static final int MAX_BALLOTS = 150000;

    /**
     * Candidate ID value to use for non-transferable ballot papers
     *
     * @design A special candidate ID value is used to indicate non-transferable
     *         votes i.e., when the list of preferences has been exhausted and
     *         none of the continuing candidates are in the preference list, the
     *         ballot is deemed to be non-transferable.
     * @see <a href="http://www.cev.ie/htm/tenders/pdf/1_2.pdf"> Department Of
     *      Environment and Local Government, Count requirements and Commentary an
     *      Count Rules, section 7, pages 23-27</a>
     */
    public static final int NONTRANSFERABLE = 0;

    /** List of candidates in order of preference */
    // TODO protected invariant preferenceList.owner == this;
    protected/*@ spec_public non_null */int[] preferenceList;

    /** Total number of valid preferences on this ballot paper */
    protected/*@ spec_public @*/int numberOfPreferences;

    /** Position within preference list */
    protected/*@ spec_public @*/int positionInList;

    /**
     * Generate an empty ballot paper for use by a voter.
     */
    /*@ also public normal_behavior
      @   assignable numberOfPreferences, positionInList, preferenceList[*], preferenceList;
      @*/
    public Ballot(final/*@ non_null @*/int[] preferences) {
        numberOfPreferences = preferences.length;
        positionInList = 0;
        int index = 0;
        preferenceList = new int[numberOfPreferences];
        for (int i = 0; i < preferences.length; i++) {
            int preference = preferences[i];
            if (preference != NONTRANSFERABLE
                    && preference != Candidate.NO_CANDIDATE) {
```



```java
/** Return a new, freshly allocated indefinite iterator that
 * produces test data of type
 * int[]
 * for testing the method named by the String methodName in
 * a loop that encloses loopsThisSurrounds many other loops.
 * @param methodName name of the method for which this
 *                   test data will be used.
 * @param loopsThisSurrounds number of loops that the test
 *                           contains inside this one.
 */
//@ requires methodName != null && loopsThisSurrounds >= 0;
//@ ensures \fresh(\result);
protected org.jmlspecs.jmlunit.strategies.IndefiniteIterator
    vint$_Iter
    (java.lang.String methodName, int loopsThisSurrounds)
{
    return vint$_Strategy.iterator();
}

/** The strategy for generating test data of type
 * int[]. */
private org.jmlspecs.jmlunit.strategies.StrategyType
    vint$_Strategy
    = new org.jmlspecs.jmlunit.strategies.CloneableObjectAbstractStrategy()
        {
            protected java.lang.Object[] addData() {
                return TestDataGenerator.getIntArrayAsObject();
            }

            //@ also
            //@ requires o$ != null;
            protected Object cloneElement(java.lang.Object o$) {
                int[] down$
                    = (int[]) o$;
                return down$.clone();
            }
        };

/** Return a new, freshly allocated indefinite iterator that
 * produces test data of type
 * election.tally.Ballot
 * for testing the method named by the String methodName in
 * a loop that encloses loopsThisSurrounds many other loops.
 * @param methodName name of the method for which this
 *                   test data will be used.
 * @param loopsThisSurrounds number of loops that the test
 *                           contains inside this one.
 */
//@ requires methodName != null && loopsThisSurrounds >= 0;
//@ ensures \fresh(\result);
```

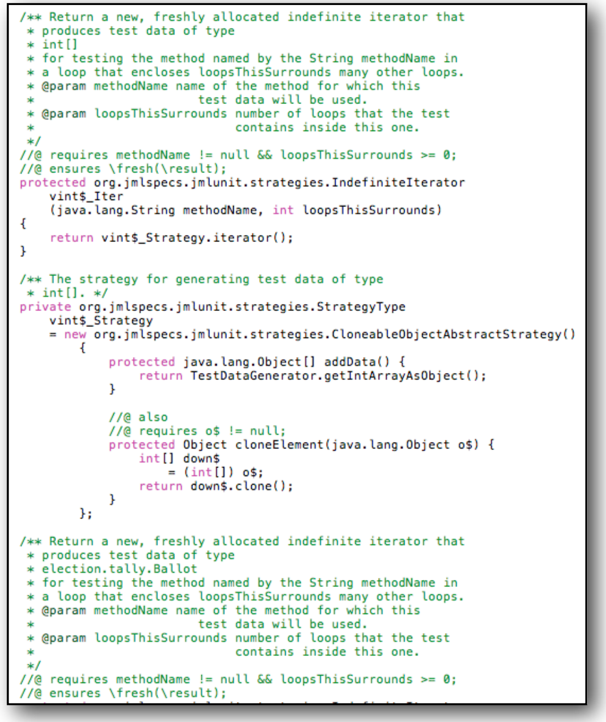
90% coverage

Unit Testing from Specs



90% coverage with only a dozen system tests

Manual System Testing from Law



```
/** Return a new, freshly allocated indefinite iterator that
 * produces test data of type
 * int[]
 * for testing the method named by the String methodName in
 * a loop that encloses loopsThisSurrounds many other loops.
 * @param methodName name of the method for which this
 *                   test data will be used.
 * @param loopsThisSurrounds number of loops that the test
 *                           contains inside this one.
 */
//@ requires methodName != null && loopsThisSurrounds >= 0;
//@ ensures \fresh(\result);
protected org.jmlspecs.jmlunit.strategies.IndefiniteIterator
    vint$_Iter
    (java.lang.String methodName, int loopsThisSurrounds)
{
    return vint$_Strategy.iterator();
}

/** The strategy for generating test data of type
 * int[]. */
private org.jmlspecs.jmlunit.strategies.StrategyType
    vint$_Strategy
    = new org.jmlspecs.jmlunit.strategies.CloneableObjectAbstractStrategy()
        {
            protected java.lang.Object[] addData() {
                return TestDataGenerator.getIntArrayAsObject();
            }

            //@ also
            //@ requires o$ != null;
            protected Object cloneElement(java.lang.Object o$) {
                int[] down$
                    = (int[]) o$;
                return down$.clone();
            }
        };

/** Return a new, freshly allocated indefinite iterator that
 * produces test data of type
 * election.tally.Ballot
 * for testing the method named by the String methodName in
 * a loop that encloses loopsThisSurrounds many other loops.
 * @param methodName name of the method for which this
 *                   test data will be used.
 * @param loopsThisSurrounds number of loops that the test
 *                           contains inside this one.
 */
//@ requires methodName != null && loopsThisSurrounds >= 0;
//@ ensures \fresh(\result);
```

for every unique election outcome

System Testing from Law

A Formal Model of Voting

A Parameterized Formal Model of Several Voting Schemes

```
-- An individual person standing for election
sig Candidate {
 votes:           set Ballot,   -- First preference ballots assigned to this candidate
   transfers: set Ballot,  -- Second and subsequent preferences received
   surplus:        set Ballot,    -- Ballots tranferred to another candidate election
 wasted:           set Ballot,  -- Ballots non-transferable due to exhaustion of preferences
   outcome:      Event            -- Election result for candidate and associated ballots
} {
   // Non-transferable ballots
   0 < #wasted implies (outcome = WinnerNonTransferable or
                       outcome = QuotaWinnerNonTransferable or
                       outcome = EarlyLoserNonTransferable or
                         outcome = SoreLoserNonTransferable)
   (outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
    implies wasted in surplus
   (outcome = EarlyLoserNonTransferable or outcome = SoreLoserNonTransferable)
    implies wasted in votes + transfers
   // Division of ballots into first preferences and transfers
     no b: Ballot | b in votes & transfers
   // Division of ballots into piles for each candidate
     all b: Ballot | b in votes + transfers implies this in b.assignees
   // Selection of surplus ballots for re-distribution
     surplus in votes + transfers
     Election.method = Plurality implies #surplus = 0 and #transfers = 0
     0 < #transfers implies Election.method = STV
   // Calculation of surplus for PR-STV election
   ((outcome = Winner and Election.method = STV) or (
    outcome = SurplusWinner or outcome = WinnerNonTransferable)) implies
    Scenario.quota + #surplus = #votes
     (outcome = Winner or outcome = SurplusWinner or
    outcome = WinnerNonTransferable) implies #transfers = 0
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies surplus in transfers
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies
         Scenario.quota + #surplus = #votes + #transfers
     0 < #surplus implies (outcome = SurplusWinner or outcome = AboveQuotaWinner or
                      outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
     (outcome = EarlyLoser or outcome = TiedEarlyLoser or
    outcome = EarlyLoserNonTransferable) iff
          (this in Scenario.eliminated and
    not (#votes + #transfers < Scenario.threshold))
     // All non-sore losers are at or above the threshold
   outcome = TiedLoser implies Scenario.threshold <= #votes + #transfers
```

Alloy Model

Table 1 gives – as an example – the numbers from the multi-member constituency of Østjylland (Eastern Jutland).

1.2.2. Step Two: Determining of Passing the Threshold

This step determines which parties are eligible for compensatory seats. This is done by checking if participating parties meet any of three requirements. Thus, the Danish electoral system has not one, but three different electoral thresholds, and parties qualify for participation in the allocation of compensatory seats by any one of them. The three thresholds are:

1. winning a seat directly in any of the ten multi-member constituencies;
2. obtaining in two of the three electoral provinces a number of votes corresponding – at least – to the provincial votes/seat ratio (using in the calculation of these ratios the number of seats in the multi-member constituencies in the electoral provinces in question, excluding the provinces' compensatory seats); or
3. 2 per cent of the valid, national vote.

For parties that do not meet the first requirement (in 2007 it was two of nine participating parties), the relevant numbers are shown in Table 2, which allows a comparison of thresholds (2) and (3), and the votes for the two parties in question in the three electoral provinces as well as nationally.

Experience shows that threshold (3), the 2 per cent rule, is much more important than threshold (2), the vote/seat ratio in two of three electoral provinces. Parties that meet the 2 per cent requirement will often also have met threshold (2) – as was the case in 2007 with the Unity List – while parties below the 2 per cent hurdle almost invariably will not meet any of the other requirements (as shown by the example of the Christian People's Party in 2007, which failed to cross any of the three thresholds). This experience illustrates how Danish political parties are not (any longer) primarily local or provincial in their support patterns.

1.2.3. Step Three: Allocating Compensatory Seats to Parties

This is the decisive step, since it is here that the proportional, overall, national (or upper-tier) allocation of all 175 seats takes place. The calculation (reproduced in Table 3 below) allocates the seats available to parties which have qualified for participation in this allocation in strict proportionality to the number of votes obtained by these parties. The calculation is done on the basis of the so-called pure Hare quota; seats not allocated by the full

Table 2. How the Parties that Failed to Qualify for Seats at Threshold (1) Fared on Threshold (2) and (3). November 13, 2007.

	All of Denmark	Metropolitan Copenhagen	Sealand-Southern Jutland	Northern and Central Jutland
Threshold 2:				
Valid votes per multi-member constituency seat	n.a.	26,906	25,103	25,146
Threshold 3:				
2 per cent of valid national votes	69,189	-	-	-
The Parties' Votes:				
K. Christian People's Party	30,013	5,513	7,635	16,865
Y. New Alliance	97,295	40,241	30,358	26,696

```
-- An individual person standing for election
sig Candidate {
 votes:        set Ballot,   -- First preference ballots assigned to this candidate
   transfers: set Ballot,  -- Second and subsequent preferences received
   surplus:        set Ballot,     -- Ballots tranferred to another candidate election
 wasted:           set Ballot,  -- Ballots non-transferable due to exhaustion of preferences
   outcome:      Event            -- Election result for candidate and associated ballots
} {
   // Non-transferable ballots
   0 < #wasted implies (outcome = WinnerNonTransferable or
                  outcome = QuotaWinnerNonTransferable or
                  outcome = EarlyLoserNonTransferable or
                    outcome = SoreLoserNonTransferable)
   (outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
     implies wasted in surplus
   (outcome = EarlyLoserNonTransferable or outcome = SoreLoserNonTransferable)
     implies wasted in votes + transfers
   // Division of ballots into first preferences and transfers
     no b: Ballot | b in votes & transfers
   // Division of ballots into piles for each candidate
     all b: Ballot | b in votes + transfers implies this in b.assignees
   // Selection of surplus ballots for re-distribution
     surplus in votes + transfers
     Election.method = Plurality implies #surplus = 0 and #transfers = 0
     0 < #transfers implies Election.method = STV
   // Calculation of surplus for PR-STV election
   ((outcome = Winner and Election.method = STV) or (
     outcome = SurplusWinner or outcome = WinnerNonTransferable)) implies
     Scenario.quota + #surplus = #votes
     (outcome = Winner or outcome = SurplusWinner or
    outcome = WinnerNonTransferable) implies #transfers = 0
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies surplus in transfers
     (outcome = QuotaWinner or outcome = AboveQuotaWinner or
    outcome = QuotaWinnerNonTransferable) implies
        Scenario.quota + #surplus = #votes + #transfers
     0 < #surplus implies (outcome = SurplusWinner or outcome = AboveQuotaWinner or
                    outcome = WinnerNonTransferable or outcome = QuotaWinnerNonTransferable)
     (outcome = EarlyLoser or outcome = TiedEarlyLoser or
    outcome = EarlyLoserNonTransferable) iff
          (this in Scenario.eliminated and
    not (#votes + #transfers < Scenario.threshold))
      // All non-sore losers are at or above the threshold
   outcome = TiedLoser implies Scenario.threshold <= #votes + #transfers
```

Law-Alloy Refinement

Rigorous System Test Generation

scenario

candidate

ballot

Core Concepts of Elections

event

method

election

Core Concepts

- candidate
  - votes (set of ballots)
  - transfers (set of ballots)
  - surplus (set of ballots)
  - outcome (event)
- ballot
  - assignees (set of candidates)
  - preferences (sequence of candidates)

Core Concepts

- scenario
  - losers (set of candidates)
  - winners (set of candidates)
  - eliminated (set of candidates)
  - threshold (integer minimum # of votes to not be a sore loser)
  - quota (integer minimum # of votes for an STV or quota winner)

Core Concepts

- event, exactly one of...
  - Winner, QuotaWinner, CompromiseWinner, TiedWinner, TiedLoser, Loser, TiedEarlyLoser, EarlyLoser, TiedSoreLoser, SoreLoser
- election
  - candidates (set of candidates)
  - seats (integer)
  - method (plurality or STV)
  - ballots (integer # of unspoiled ballots)

Generating Scenarios

- goal: generate and characterize every possible non-isomorphism scenario
  - election method, # candidates, # seats
- example outcomes
  - WL or <u>WL</u> in two candidate plurality
  - SSSLLLL<u>LLW</u> with 10 candidates and 1 seat in STV
- scenarios as lemmas
  - “I bet there can’t be an election outcome like this!”

Coupling Systems

- couple Alloy to jUnit
- generate and save system tests in generic format for reuse across implementations
- perform code coverage analysis
- characterize system correctness
- identify suspicious parts of an implementation

Ongoing Results

- generated all scenarios for up to 7 candidates in PR-STV using several months of CPU time
- 99.9% code coverage
- early results after only two days of CPU time detected two cases missed in scenario analysis
- zero bugs detected in verified counting system

Summary of Current Affairs

- formally specified, validated, and verified election tally software systems for US, NL, IE, and DK
- traceable refinement from law—interpreted as concepts, features, and requirements—to specifications, software, and proofs
- automatic verification using ESC/Java2
- automated unit tests with 97% coverage
- manual system tests with 97% coverage
- automated system tests with 100% coverage
- all research and development done in "spare time"

Next Steps

- formal model of elections
  - system model that includes people, parties, bureaucrats, government
- trust-by-design
  - software engineering in the face of an adversarial customer (gov. and citizens)
- logic-based voting scheme
  - couple LFs to implementation

Danish Council for Strategic Research
Programme Commission on
Strategic Growth Technologies

5 years
17M direct
32M total

DemTech

Basin (ETHZ)
Ryan (Lux)

Fredericksberg
Aarhus
Copenhagen

Siemens
Aion Assembly

Schürmann
Kiniry
Markussen

Thanks to Collaborators

- KOA
  - Dermot Cochran, Fintan Fairmichael, Engelbert Hubbers, Alan Morkan, Martijn Oostdijk
- Vótáil
  - Dermot Cochran
- DiVS
  - Dermot Cochran, Ólavur Kjølbro

See DemTech.dk
for more information