

Group machine decomposition by coupled cyclic groups

NICO F. BENSCHOP – *Amspade Research, The Netherlands*¹

Abstract: Finite State Machine $M(Q, A)$ with stateset Q and input alphabet A (known as a Moore machine), and its *Sequential Closure* (semigroup) $S = A^*/Q$ are introduced, recalling basic principles in theory and practice. State machines with isomorphic closures are defined equivalent. Each finite semigroup S can be represented by at most $|S| + 1$ states, viz. itself, possibly extended by a left-identity. So state set Q can be expanded to semigroup S to represent M . It is shown that a right congruence of S is sufficient for cascade decomposition of M . This applies also to decompose a permutation machine with a non-cyclic simple group as closure, which is indecomposable by the known Krohn/Rhodes decomposition [6][7]. As illustration, the smallest non-cyclic simple group A_5 of order 60 is decomposed as a state machine network of coupled cyclic groups (periodic counters) of order 2 (twice), 3 and 5.

Keywords: Automaton, state machine, permutation, simple group, semigroup, right-congruence, preserved partition, cascade, coupling, cyclic group.

1 Coupling State Machines

Two state machines may be coupled by a combinational function mapping the state set of one machine, combined with external input, into the input set of the other machine. Three ways of coupling two component state machines into a network of parallel operating machines are:

- no coupling or 'independent' composition (*direct product*)
- one-way coupling or 'cascade' composition (*coupled product*)
- both-way coupling or 'loop' composition (*loop product*)

Loopfree decomposition of a state machine depends on an algebraic property of its sequential closure, in order to hold for all possible input sequences. It is referred to as a 'congruence' on the semigroup, or 'preserved partition' [5] of the state set representing the machine's behaviour.

Loop composition turns out to be superfluous, and in fact is undesirable for practical engineering purposes, since it requires more coupling logic than necessary. A *loopfree* composition suffices in all cases, applying the first two types of coupling, of which the second (cascade coupling) is required only for non-commutative systems, illustrated by some typical examples :

- (a) the 'symmetric group' S_3 of all six permutations of 3 states,
and S_4 of the $24 = 4!$ permutations of 4 states.
- (b) the smallest noncyclic simple group:
'alternating group' AG_5 of all 60 even permutations of 5 states.

In Krohn/Rhodes' theory [6] of 1965 permutation machines with a non-cyclic simple group as closure are (rather complex) indecomposable basic components. It is shown that, by a coupling mechanism different from their 'wreath product', such permutation machines can be decomposed into a network of coupled cyclic groups. The absence of recent references may be excused, since this incompleteness aspect of their theory has thus far gone unnoticed.

¹Drossaardstraat 71, 5663GJ Geldrop, The Netherlands (nfbenschop@onsbrabantnet.nl)

2 Machine decomposition: right congruence suffices

Generative state machine representation of semigroups causes a sequential *asymmetry of time* corresponding to a right congruence, or preserved state partition [5], to be sufficient for inducing a cascade decomposition. This applies also to closures without a full congruence such as non-cyclic simple groups, which do have subgroups and as many right congruences.

In fact each *subgroup* $H \subset G$ defines, by equivalencing it, a unique *r-congruence* ([2]-p31) of disjoint right cosets Hx ($x \in G$).

Def 2.1: To each subgroup $H \subset G$ of a simple group $G = \{g_i\}^*$ corresponds a left- and right congruence pair that is orthogonal, in the sense that: $Hg_i \cap g_iH \equiv g_i$ for generators g_i .

Notation : A^* is the (infinite) set of non-empty strings over alphabet A , and A^*/Q is the generated (finite) closure of distinct transformations of Q ,

with equivalence in A^* : $x \equiv y \pmod{Q} \iff qx = qy$ for all $q \in Q$. In other words, two input strings are equivalent (mod Q) if they have equal effect on machine M .

Quantification and optimization are dominant aspects of engineering, so the next concepts are relevant for practical synthesis of sequential machines :

Def 2.2: The dimension of machine $M(Q, A)$ is the smallest number of generators of its closure $S_M = A^*/Q$: $\dim(M) = \dim(S_M) = |A|_{min}$.

Def 2.3: The degree of M and S_M is the smallest number of states to represent S_M by distinct state transforms : $\deg(M) = \deg(S_M) = |Q|_{min}$.

For example $\dim(C_6)=1$ with $\deg(C_6)=5$ (the sum of its coprime factors $6=2.3$), and the full group FG_3 of all six permutations of 3 states has: $\dim(FG_3)=2$ and $\deg(FG_3)=3$. Although FG_3 is represented over only 3 states, its decomposition as a coupled network of two cycles C_2 and C_3 (see next section) is possible by *expanding* state set Q to the group itself.

LEMMA 2.1 *Each finite semigroup S can be represented by a state machine of at most $|S| + 1$ states.*

PROOF. A semigroup S can act as state set $Q = S$ for its representation by a state machine if the square $|S| \times |S|$ composition table of S has distinct columns, so for each pair $x \neq y \in S$: $qx \neq qy \in S$ for some $q \in S$.

If equal columns do occur, as for instance in a left-copy semigroup: $ab \equiv a$ for all $a, b \in S$, then only one extra state q_0 suffices to obtain distinct columns, while preserving semigroup structure, by defining $q_0 x \equiv x$ for all $x \in S$, with $Q = \{S, q_0\}$ hence $|Q| = |S| + 1$. \square

If a state set Q of less than $|S|$ states represents S , so $|Q| = \deg(S) < |S|$, then there is a right congruence ρ on S , and parts S/ρ are the states in Q .

Def 2.4: A *defining* right congruence δ of S has $|S/\delta| = |Q| = \deg(S)$ parts, which function as the states of a representation of S over Q .

By the left-to-right *asymmetry* of state-transform composition (input sequencing), the state machine representation of a semigroup S implies:

LEMMA 2.2 *Let δ be a defining r-congruence of semigroup S , then: a r-congruence $\rho > \delta$ induces a cascade decomposition of S .*

PROOF. Let subset A generate S , and machine $M(Q, A)$ has closure S , represented over state set $Q = S/\delta$ with $|Q| = \deg(S)$. Then a right congruence $\rho > \delta$ on S , with $q \equiv r \in S \iff qa \equiv ra$

(mod ρ) for all $a \in A$, is a preserved state partition. The corresponding cascade decomposition of $M(S, A)$ has $Q_1 = S/\rho$ as state set of leading component $M_1(Q_1, A_1)$ with $|Q_1| < \text{deg}(S)$. Input set $A_1 = A/\rho$ equivalences inputs of A that induce the same Q_1 transformation in M_1 , hence: $a \equiv b \in A \pmod{A_1} \iff qa \equiv qb \in Q_1 \pmod{\rho}$ for all $q \in S$.

So all states in the same ρ -part map under any input into the same 'next-state' ρ -part.

Hence ρ is called a preserved partition, and the ρ -parts represent the component states in $Q_1 = S/\rho$ of image machine $M_1(Q_1, A_1)$ with input set $A_1 = A/\rho$.

In case one extra initial state q_0 is required (lem2.1) for true representation of S by $M(Q, A)$ - where $Q = \{S, q_0\}$ - then 'right-congruence' of S is replaced by 'preserved partition' of Q . \square

So a full (left- and right-) congruence is not needed for cascade decomposition, contrary to the known automaton decomposition of Krohn–Rhodes [6]. This allows simple groups, with no full congruence resp. normal subgroup, to be decomposed as permutation machine (section 5).

Denote the ρ -part of state q by $\rho(q) = q_1$, thus as the first component of some state coding.

Then the preserved property of the r-congruence ρ is expressed by: $q_1a = (qa)_1$ for all $a \in A$.

In other words, under any input a the ρ -part q_1 of any state q maps into the ρ -part of its next state qa , so :

$$\rho(qa) = \rho(q)a \quad \text{for all } q \in Q \quad \text{and all } a \in A.$$

Let $\rho(a)$ denote the corresponding ρ -part a_1 of input a , with equivalence :

$$\rho(a) = \rho(b) \text{ for } a, b \in S \text{ defined by: } a_1 = b_1 \iff q_1a \equiv q_1b \text{ for all } q_1 \in Q_1.$$

Then by associativity of input- resp. transform composition in $S = A^*/Q$:

$$\rho(qx) \equiv \rho(q) \rho(x) \text{ for all } q \in Q, x \in S. \tag{1}$$

This composition property is a r-congruence ρ of S , apparently sufficient for cascade machine decomposition.

Notice that in a *commutative* system S the r-congruence yielding an image system S_1 , resp. leading machine component M_1 , is also l-congruence, hence a full congruence. For instance $Z_{10}(\cdot)$ is represented over 6 states with defining congruence $\rho : \{2=7, 4=9, 8=3, 6=1; 5; 0\}$ given by two subsemigroups $Z_5=\{2, 4, 8, 6; 0\}$ and $Z_2=\{5; 0\}$, with $Z_{10} \cong Z_5 \times Z_2$, the direct product of Z_5 and Z_2 , requiring no coupling function between them.

3 Cascade composition: full groups FG_3 and FG_4

Recall a *group* G_n of permutations of n objects (states) is an associative closure with just one idempotent element e , the group identity [1] [2]. And each element $a \in G_n$ has a unique inverse a^{-1} with respect to e such that $a a^{-1} = a^{-1} a = e$. For finite n the iteration class a^* of all iterations a^i of a is a cyclic subgroup of G_n : $\text{dim}(a^*) = 1$. Iterations a^i must eventually yield $a^{m+1} = a$ for some $m \leq |G_n|$, hence $a^m = e$ with inverse $a^{-1} = a^{m-1}$, and m is the order (or rather period) of a in G_n .

There are $n! = \prod_{i=1}^n i$ (n factorial) permutations of n states, usually referred to as the 'symmetric group' S_n of degree n . However, in this context S is reserved for 'semigroup' and *Sylow* p -subgroup, so the term full group FG_n is preferred.

Consider full group FG_3 of all 6 permutations of 3 states, generated by two permutations a and b of order 3 and 2. This group is isomorphic to the group of symmetries of an equilateral triangle, thus with sides of equal length. The three states 1, 2, 0 then represent the three corners, and

permutation a in the next table maps $\{1 \rightarrow 2, 2 \rightarrow 0, 0 \rightarrow 1\}$, a rotation of 120° generating a 3-cycle: $a^3 \equiv e$.

MFG3: a b	aA	bA	aA^2	bA^2	Structure:
1	2 0	0 2	1 1	1 1 0 2	C2 > C3
2	0 2	1 1	0 2	2 0 2 0	
0	1 1	2 0	2 0	0 2 1 1	e=bb=aaa
					ab ba e e ba b a ab aa a b
Q	A	-- A^2 --	----- A^3 -----		

Figure 1: State machine M_{FG_3} generating the full group FG_3 of order 6.

The figure shows state machine transition table $M_{FG_3}(Q, A)$ with $Q = \{1, 2, 0\}$, input alphabet $A = \{a, b\}$ and the permutations of Q , noted as columns, generated by all input sequences A^* over A . The sequences over A of increasing length k are lexically generated by recursive prefixing: $A^{k+1} = A A^k = \{aA^k, bA^k\}$. For the resulting Q -transforms, simply copy the rows of A^k to positions of A^{k+1} indicated by A , thus implementing function composition $q(xy) \equiv (qx)y$ for all $x, y \in A^*$, $q \in Q$.

In the example: $A^3 \equiv A \cup A^2 \pmod{Q}$, meaning that strings of length 3 produce no new permutations of Q . Hence none are produced by longer strings, completing the generation process of group FG_3 . Clearly FG_3 is non-commutative since $ab \not\equiv ba$, in fact arithmetically: $ab \equiv ba + 1 \pmod{3}$.

Notice transformation $a : q \rightarrow q + 1 \pmod{3}$ for each $q \in Q$. So a^* has the structure of $Z(+)$ mod 3 with $Q = \{1, 2, 0\}$ as residues, denoted $a^*/Q \cong Z_3(+)$, or briefly: 3-cycle $C_3 \cong a^*/Q$. And b swaps 0 and 1 while fixing state 2, in effect $b^*/Q \cong Z_2(+)$ $\cong C_2$. For known context the notation $/Q$, or mod Q , may be omitted if no confusion arises.

Now $\text{deg}(FG_3)=3$ with defining r-congruence $\delta : \{b \equiv e, ba \equiv a, ba^2 \equiv a^2\}$, generated by the r-consequences of equivalence $b \equiv e$, thus equivalencing subgroup C_2 , right-composed by the iterations a^i of a . This 3-state model of FG_3 has no preserved state partition, verified by equivalencing any state-pair and noting the right consequences by comparing the two corresponding rows position wise. Then all states are equivalenced as a trivial one-part r-congruence. In fact :
 – representation over a minimal state set *hides* structural decompositions.

Taking FG_3 itself as state set shows a r-congruence $\rho : \{a^*, [a^*]b\}$, yielding a cascade network of two coupled cycles, with r-image $C_2 = FG_3/\rho$ as independent component, and subgroup C_3 as dependent component, seen as follows (see fig.2).

The three elements of period 2, namely b, ab, ba (fixing state 2, 0, 1 respectively) form with identity e three subgroups C_2 of order 2. While a and a^2 of period 3 form with e one subgroup C_3 . Equivalencing $a \equiv a^2 \equiv e$ yields, upon right composition by b , the equivalences $ab \equiv a^2b \equiv b$, where $a^2b \equiv ba$. These two parts $a^* = [a, a^2, e]$ and $[a^*]b = [ab, ba, b]$ form a congruence ρ with corresponding r-image group $FG_3/\rho \cong C_2$. The two ρ -parts behave as states in the 2-cycle of leading machine component C_2 .

To model the non-commutativity of FG_3 , the *coupling function* between these two components is found by first considering their direct product $C_2 \times C_3$. Then permute component C_3 internally by an automorphism $\alpha : C_3 \rightarrow C_3$ into a dependent component $[C_3]'$ of the same structure. This way the total number of product elements remains the same, while the (coupling-) twist implements the non-commutative structure of $G = FG_3$.

Associativity $q(xy) = (qx)y \in Q = G$ for all $q, x, y \in G$ follows from the two components in $G = G_1 \triangleright G_2$, having element codes $q=[q_1, q_2]$, $x=[x_1, x_2]$, $y=[y_1, y_2]$ with $\{q_1, x_1, y_1\} \in G_1$ and $\{q_2, x_2, y_2\} \in G_2$. First component G_1 behaves independently from the second (dependent) component G_2 , so the associative property of G is preserved in its image G_1 , and only the second component needs verification.

Denote as α_{x_1} the automorphism $G_2 \rightarrow G_2$ induced by a particular first component value x_1 , and similarly define α_{y_1} . The twisted x_2 and y_2 are $x'_2 = \alpha_{x_1} x_2 \alpha_{x_1}^{-1}$ and $y'_2 = \alpha_{y_1} y_2 \alpha_{y_1}^{-1}$. Then associativity of the coupled network follows from :

$$[q(xy)]_2 = q_2 (x'_2 y'_2) = q_2 (\alpha_{x_1} x_2 \alpha_{x_1}^{-1} \alpha_{y_1} y_2 \alpha_{y_1}^{-1}) = (q_2 x'_2) y'_2 \quad (2)$$

because q_2, x'_2, y'_2 as elements of G_2 compose associatively.

The coupling from C_2 to C_3 is established by identifying each element of C_2 with an automorphism of $C_3 = \{1, 2, 0\}$ of which there are two namely $\alpha : [swap(1, 2), fix(0)]$ and identity mapping $\alpha^2 = \epsilon : fix(1, 2, 0)$.

Such coupling map: $C_2 \rightarrow aut[C_3]$ can be chosen in various ways. For instance the trivial map of C_2 onto the identity of $aut[C_3]$, hence no 'twist' and in effect no coupling, yields the direct product as special case.

Note 3.1: Distributive property $(a + b)c = ac + bc$ of multiplication mod m represents the semigroup of all endo-morphisms of addition mod m , so: $Z_m(.) \cong endo[Z_m(+)]$. The automorphisms of $Z_m(+) \cong C_m$ are the invertible endo-morphisms. So the units group of $Z_m(.)$ consists of all residues coprime to m , operating as multipliers (mod m) on residues in $Z_m(+)$.

By $C_3 \cong Z_3(+)$ and $endo(C_3) \cong Z_3(.)$ the subgroup $C_3 = \{1, 2, 0\} \cong \{a, a^2, e\}$ of FG_3 has automorphisms $\alpha : \{swap(1, 2), fix(0)\}$ and $\alpha^2 = \epsilon : fix(1, 2, 0)$ which form the cyclic group $C_2 \cong \{\alpha, \alpha^2\}$ of order 2.

The coupling function swaps 1 and 2 (a and a^2) in C_3 to obtain twisted dependent component $[C_3]'$ in semi-direct product, or 'coupled product' $FG_3 \cong C_2 \triangleright C_3$ with coupling $\gamma : C_2 = [1, 0] \rightarrow aut(C_3) = \{\alpha, \epsilon\}$.

Notice $baa \equiv ab$, $aba \equiv b$, $aab \equiv ba$, $bab \equiv aa$, with 2-component code (fig.2) :
 $a = [0, 1]$ $a^2 = [0, 2]$ $e = [0, 0]$ and $ab = [1, 1]$ $ba = [1, 2]$ $b = [1, 0]$.

Similar to direct product $C_2 \times C_3$ for cyclic group C_6 , composition of elements in FG_3 is done component wise using a twisted $[C_3]'$, denoted $C_2 \triangleright C_3$ with coupling map $\gamma : C_2 \rightarrow aut[C_3]$, called *semidirect-* or *coupled product* of semigroups, or *cascade composition* of state machines.

Notice the coupling map: $[swap(1, 2) fix(0)] \text{ mod } 3$ is a multiplication by 2 (mod 3) in C_3 if the C_2 component is in state 1, and uncoupled (direct) composition $z_2 \equiv x_2 + y_2 \text{ (mod } 3)$ with C_2 component in state 0.

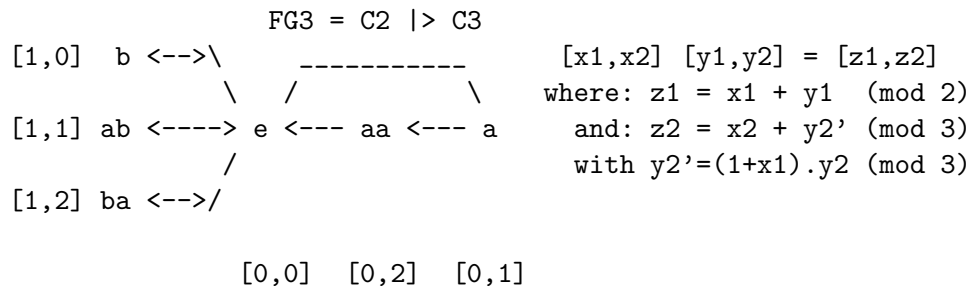


Figure 2: Iterative and arithmetic coupling structure of full group FG_3

In summary, this method couples two groups: $G_1 \triangleright G_2 \cong G$ where G is the *sequential product* $G = G_1 G_2$ of two orthogonal subgroups G_1 and G_2 so $G_1 \cap G_2 = e$ with coupling $\gamma : G_1 \rightarrow \text{aut}(G_2)$ mapping image G_1/γ to a subgroup of $\text{aut}(G_2)$. Essential is :

No full congruence on G is required for its decomposition.

A right-congruence suffices (i.e. a subgroup = r-congruence part with identity e)

Notice in product $G = G_1 G_2$ of *orthogonal* groups G_1 and G_2 (intersecting only at e) the multiplicity of one factor, as subgroup $G_i \subset G$, is the order $|G_j|$ of the other, and 1 for the other factor G_j as subgroup of G . So either G_1 occurs $|G_2|$ times in G , and G_2 just once, or v.v. In both cases the total order is $|G| = (|G_1| - 1)|G_2| + |G_2| = (|G_2| - 1)|G_1| + |G_1| = |G_1| |G_2|$.

Due to $Z_n(\cdot) \cong \text{aut}(C_n)$, coupling $C_m \triangleright C_n$ of two cycles requires $C_m/\gamma \subseteq \text{units group of } Z_n(\cdot)$ for some (possibly trivial 1-1) congruence γ of C_m . So for prime cycles $C_p \triangleright C_q$ (primes $p < q$) : p must divide $q - 1$.

This is the basis of a completely **arithmetic model** of permutation machines, viz. sequential behaviour with a group as closure. Recall to each subgroup $H \subset G$ of a finite group G corresponds a unique r-congruence $\rho(H)$: equivalence all elements of H , then the right consequences yield the r-cosets Hx of H in G , forming the parts of $\rho(H)$. [2]-p10.

Consider finite group $G = HK$ of composite order as sequential product of subgroups H and K , where $H \cap K = e$, the identity of G . So each $x \in G$ has form $x = hk$ for a unique pair $h \in H$, $k \in K$, both in G .

Right congruence $\rho(H)$ and left congruence $\lambda(K)$ are *orthogonal*, with each element of G determined by its ρ - and λ - part. Such product always exists, since a group G of composite order has a proper subgroup $H \subset G$, generating r-congruence ρ of disjoint r-cosets Hx , orthogonal to $\lambda(K)$ of left-cosets xK generated by subgroup K with one element in each $\rho(H)$ -part, and vv.

Def 3.1: Coupled Product (CP) of permutation machines.

Let permutation machine M_G generate product group $G = HK$ (subgroups $H, K \subset G$) with $H \cap K = e$. Then G is a coupled product $G = H \triangleright K$, with *cascade* machine composition $M_G = M_H \triangleright M_K$, if a **coupling map** $\gamma : H \rightarrow \text{aut}(K)$ exists, permuting K into $K' \cong K$ by $k' = \gamma_h(k)$. Here γ maps (not nec. 1-1) image group H/γ onto a subgroup of $\text{aut}(K)$.

LEMMA 3.1 *Composing prime-order cyclic groups* $C_p \triangleright C_q$:

$C_p \cong Z_p(+)$ and $C_q \cong Z_q(+)$ (primes $p < q$) have a non-trivial coupled product (CP) via $\gamma : C_p \rightarrow \text{aut}(C_q) \cong Z_q(\cdot) \setminus 0 \cong C_{q-1}$ **iff** $p \mid (q - 1)$.

PROOF. Coupling function γ maps C_p into $\text{aut}(C_q) \cong C_{q-1}$, and $h \in C_p$ has image $\gamma_h = h' \in \text{aut}(C_q)$ which as multiplier $k' = k h'$ (k, k' in C_q) represents an automorphism of C_q . Prime cycle C_p has only itself as non-trivial image group $C_p/\gamma = C_p$, hence p must divide $q - 1$. Conversely $p \mid (q - 1)$ allows $\gamma : C_p \rightarrow \text{aut}(C_q) \cong C_{q-1}$ for coupling purposes. \square

COROLLARY 3.1 *For primes* $p < q$, *with* p *not dividing* $q - 1$, *two cyclic components* C_p *and* C_q *cannot be composed into a non-commutative group by a coupled product (CP) in either direction. The only possible composition is direct product* $G \cong C_p \times C_q \cong C_{pq}$, *which is cyclic and commutative.*

4 Decomposing the full- and alternating group over four states

The full group FG_4 of all $24 = 4!$ permutations of 4 states $Q = [1, 2, 3, 0]$ requires only 2 generators of periods 4 and 2, as shown in fig 3a. Only irreducible 'new' strings are used

for extension from A^k to A^{k+1} . Counting the number of new elements (\wedge) per A^k yields a generative spectrum $[2,4,5,5,5,3]$ characteristic for FG_4 . Their sum is the group order.

Def 4.1: In group G/Q the stabilizer V_q of state $q \in Q$ consists of the transformations fixing state q , forming a subgroup of G . By symmetry: all n stabilizers of FG_n are isomorphic to FG_{n-1} of order $(n-1)!$

The intersection of two stabilizers fixes the **union** of their fixed states.

In FG_4 each stabilizer $V_q \cong FG_3$ has order 6, which occurs four times.

For instance state 0 is fixed by $\{ab, e, x, r, m, n\} = V_0 \cong FG_3$ (fig a)

where $e \equiv bb$, $x \equiv (ab)^2$, $r \equiv aaaba \equiv a^{-1}ba$, $m \equiv aabaa$, $n \equiv baaab$

with identity e , while ab, x have period 3, and r, m, n have period 2.

The defining r-congruence δ of FG_4 is formed by the r-cosets of any stabilizer, say $V_0 \cong FG_3$ with $\delta = \{V_0, V_0a, V_0a^2, V_0a^3\}$ and $a^*/Q \cong C_4$.

Note 4.1: By the stabilizer concept and induction, each finite full group FG_n over $|Q| = n > 2$ states is generated by only two permutations a, b of periods n and 2, with $a^*/Q \cong Z_n(+)$ $\cong C_n$, and $b = [swap(0, 1), fix(other states)]$ hence $b^*/Q \cong C_2$ and $a^n \equiv b^2 \equiv e$. \square

In coupled product $FG_3 = C_2 \triangleright C_3$ image $C_2 \cong FG_2$ occurs three-fold as stabilizer of the three states representing FG_3 (figs 1, 2). Similarly, four-fold stabilizer FG_3 in FG_4 yields coupled product $FG_4 = FG_3 \triangleright C_4$ (fig. 3b)

Coupling map $\gamma : FG_3 \rightarrow aut(C_4) \cong C_2$ uses image $FG_3/\gamma \cong C_2$ of even and odd permutations, the latter activating $-1 \in Z_4(.)$ as multiplier of the C_4 component to obtain its twisted version $[C_4]'$, with result:

$$\underline{cascade\ decomposition} : \quad FG_4 \cong (C_2 \triangleright C_3) \triangleright_{\gamma} C_4 \quad (3)$$

In the corresponding three-component code $x = [x_1, x_2, x_3]$ for each of the 24 elements $x \in FG_4$, the respective component values are taken mod 2, mod 3 and mod 4, hence from: $\{0, 1\}$, $\{0, 1, 2\}$ and $\{0, 1, 2, 3\}$.

To comply with this threefold structure, it is useful to consider also three generators, rather than the two that are necessary and sufficient. This better matches the recursive generation process based on sequential product $FG_{n+1} = FG_n C_{n+1} = C_{n+1} FG_n$ for any number n of states, with FG_n as stabilizer of extra state $n+1$. States and inputs are renamed for this purpose (fig 3b).

State space $[0,1,2]$ of FG_3 is expanded to $[0,1,2,3]$ for FG_4 by one extra state '3'. This new state is fixed by both generators a, b of orders 2 and 3 respectively, where $a = [swap(0, 1) fix(2, 3)]$ and $b = [cycle(0, 1, 2) fix(3)]$. Notice permutations a, b have the same structure as in FG_3 , however with one extra fixed state '3'. A third generator is full 4-cycle c which has the effect of generating FG_4 with shorter stringlengths, as depicted in fig 3b, with $e \equiv a^2 \equiv b^3 \equiv c^4$ and generative spectrum $[3,9,12]$. Reducible strings are marked by 'x', and a fixed state q by 'q<'.

Alternating group AG_4 over four states has order $4!/2 = 3.4 = 12$.

A 4-cycle permutation $d = [1, 2, 3, 0]$ with closure C_4 cannot occur in AG_4 because it is an odd permutation. By Sylow's theorem a subgroup of order 4 must exist, and $C_2 \times C_2$ is the only alternative. Now square $d^2 = [2, 3, 0, 1]$ swaps (0,2) and (1,3) hence is an even permutation, to be used next as generator c of AG_4 (fig 4). Together with another dual swap $b = [1, 0, 3, 2]$ it generates the subgroup $C_2 \times C_2 \subset AG_4$, while a third generator a has closure $a^* = C_3$ fixing one state, say '0'. Reducible strings are marked 'x', and new strings in A^k/Q yield generative spectrum $[3,6,3]$.

AG4:	a	b	c	aA	bA	cA	A ³	C2 x C2							
0	0<1	2	0<1	2	2	0	3	3	3	0	1	2	3	bc=cb	
1	2	0	3	3	3	0	0	1	2	1<2	1	2	1<0		
2	3	3	0	1	2<1	1	2	1	0	1	2	0	3	2<	e
3	1	2	1	2	0	3<3	3	0	2	0	3	3<0	1	/ \	
	C	C	C			x		x	x			b		c	
	3	2	2				e	\	/	e					
					ac=ba			bc=cb							

Figure 4: 'Alternating' group AG_4 as state machine $C_3 \triangleright (C_2 \times C_2)$

commutative behaviour of AG_4 . In a sequential composition xy this coupling x_1 to x_2, y_2 is active if $x_1 \not\equiv 0 \pmod{3}$, and disabled if $x_1 \equiv 0 \pmod{3}$. The four codes $[x_2, x_3]$ of $C_2 \times C_2$ are $[1,0]$ $[0,1]$ $[1,1]$ $[0,0]$ or briefly:

10, 01, 11, 00, with component-wise addition mod 2. The three non-zero codes are equivalent: the product of any pair yields the third element. Hence its automorphism group is FG_3 with C_3 as subgroup representing a 3-cycle rotation α of the three non-zero (b, c, bc) with $\alpha^3 \equiv \alpha^0 \equiv \epsilon$ the identity transformation, for instance in compact notation :

$$\alpha : 01 \rightarrow 10 \rightarrow 11 \rightarrow 01 \quad \text{and} \quad \alpha(00) = 00 \quad (\text{fixing code } 00), \quad \text{with} :$$

$$\text{coupling map } \gamma : x_1 = \{1, 2, 0\} \rightarrow \{\alpha, \alpha^2, \epsilon\} = C_3 \subset \text{aut}(C_2 \times C_2).$$

The 3-component code for group AG_4 , over $3+2+2=7$ states, yields the next arithmetic model of its cascade decomposition $AG_4 = C_3 \triangleright (C_2 \times C_2)$:

$$[x_1, x_2, x_3] [y_1, y_2, y_3] \rightarrow [z_1, z_2, z_3]$$

where :

$$z_1 \equiv x_1 + y_1 \pmod{3}, \quad \text{coupled by } x_1 \pmod{3} \text{ to} :$$

$$z_2 \equiv \alpha^{x_1}(x_2 + y_2) \pmod{2}, \quad z_3 \equiv \alpha^{x_1}(x_3 + y_3) \pmod{2}.$$

If leading component C_3 is in zero state $x_1 \equiv 0$, then coupling $\alpha^0 \equiv \epsilon$ is not active, resulting in uncoupled component-wise addition of x and y .

Rotation $\alpha(01) = 10$, $\alpha(10) = 11$, $\alpha(11) = 01$, $\alpha(00) = 00$ is applied 0, 1 or 2 times as α^{x_1} to direct sum $[x_2 + y_2, x_3 + y_3] \pmod{(2,2)}$. This implements the automorphism (permutation) of dependent component $C_2 \times C_2$, arithmetically modeling the non-commutative behaviour of AG_4 . For instance $ac \equiv ba \not\equiv ab$ (fig 4) is verified in this '3-code' as follows :

$$ac = [1,0,0] [0,0,1] = [1, \alpha^1(0,1)] = [1,1,0] \quad \text{and} :$$

$$ba = [0,1,0] [1,0,0] = [1, \alpha^0(1,0)] = [1,1,0] \equiv ac \quad (\text{see fig 4})$$

$$ab = [1,0,0] [0,1,0] = [1, \alpha^1(1,0)] = [1,1,1] \not\equiv ba. \quad \text{Moreover} :$$

$$ca = [0,0,1] [1,0,0] = [1, \alpha^0(0,1)] = [1,0,1] \not\equiv ac.$$

The structure of AG_4 shows a generalization of lemma 3.1. Denote the direct product $C_q \times C_q \times \dots \times C_q$ (k times) briefly as $[C_q]^k$, and let q be prime. Using a k -component code, the k unit vectors form a necessary and sufficient set of generators, so $\dim([C_q]^k) = k$ while $\deg([C_q]^k) = kq$.

Recall $[0,1]$ and $[1,0]$ generate $[C_2]^2$, or alternatively $[0,1]$ and $[1,1]$, or $[1,0]$ and $[1,1]$. Generalizing this, any subset of k non-zero codes that covers each unit vector or some non-zero multiple of it (any one of the $q-1$ non-zero elements of C_q generates C_q) also generates $[C_q]^k$. There are $q^k - 1$ non-zero k -codes, and any permutation of them yields an automorphism, so $\text{aut}([C_q]^k) \cong FG_{q^k-1}$. Now $|FG_{q^k-1}| = (q^k - 1)!$, and for any prime $p \mid (q^k - 1)!$, thus $p \leq q^k - 1$, a cyclic subgroup $C_p \subset FG_{q^k-1}$ exists (the converse of Sylow's theorem does hold

for single primes). Hence C_p can form a coupled product with direct product $[C_q]^k$ as dependent component.

COROLLARY 4.1 *For distinct primes p, q and k -fold direct product $[C_q]^k$:
A coupled product $C_p \triangleright [C_q]^k$ requires $p \leq (q^k - 1)$.*

5 Decomposing simple groups $AG_n \subset FG_n$ for $n > 4$

The described arithmetic coupled product (CP), which requires only subgroups resp. r-congruences, can be generalized to finite groups of any order as follows. Recall a group G of order $|G| = \prod (p_i)^{n_i}$ (distinct primes p_i) has subgroups S_i (not necessarily cyclic) of coprime orders $|S_i| = p_i^{n_i}$. These maximal **p-subgroups** or 'Sylow components' [2]-p39 are mutually disjoint or rather 'orthogonal', viz. intersecting only at the group identity e .

Def 5.1 : Sylow pair S_i, S_j has a compatible ordering $S_i \triangleright S_j$ when :

in case $S_j \cong C_{p_j}$: if $p_i \mid (p_j - 1)$, or for $k > 1$:

in case $S_j \cong [C_{p_j}]^k$: if $p_i \leq (p_j)^k - 1$ (k -fold direct product)

For any finite group G holds: $G = \prod S_i$ is the *sequential product* of its Sylow p -subgroups (such as $FG_3 = [b^*][a^*] = C_2C_3 \cong C_3C_2$). Then G allows coupled products (CP) for Sylow component pairs that can be compatibly ordered.

THEOREM 5.1 (*Ordered Sylow coupling*): *Let permutation machine M_G generate group G , being the sequential product of its Sylow p -subgroups S_i in some (arbitrary) ordering. Then :*

- (a) M_G is the ordered coupled product (CP) of subgroups S_i as permutation components M_i .
- (b) A coupling map: $S_i \rightarrow \text{aut}(S_j)$ exist only for compatibly ordered Sylow pairs $S_i \triangleright S_j$.
- (c) There are as many groups of order $|G|$ as there are distinct permutation machines generating a group of that order. They have different combinations of compatibly ordered Sylow pairs and corresponding distinct coupling functions.

For squarefree $|G|$ - thus a product of distinct primes $\prod p_i$ - with k prime pairs (p_i, p_j) compatibly ordered: $p_i \mid (p_j - 1)$, the 2^k combinations tend to yield distinct (non-isomorphic) groups of order $|G|$. For instance if $|G| = 30 = 2.3.5$ there are two compatible Sylow pairs (2,3) and (2,5) hence there are $2^2 = 4$ distinct such groups, just one of which is commutative, namely the direct product $C_2 \times C_3 \times C_5 \cong C_{30}$.

However $|G| = 42 = 2.3.7$ has three compatible pairs (2,3) - (2,7) and (3,7) yet only 6 groups (not $2^3 = 8$) of that order.² Due to the pair 'chain' (2,3) \rightarrow (3,7) seemingly distinct coupled structures can generate isomorphic groups, and 2^k is an upperbound to the number of distinct groups, which is reached if no such chain of compatible pairs occurs. So $|G| = 110 = 2.5.11$ with $k = 3$ and chain (2,5) \rightarrow (5,11) yields $6 < 2^3$ groups, $|G| = 105 = 3.5.7$ (3,7) and $|G| = 165 = 3.5.11$ (5,11) each yield $2^1 = 2$ groups, $|G| = 70 = 2.5.7$ with $k=2$ and no chain has $2^2 = 4$ groups.

As shown for $n \leq 4$: full group FG_n has n stabilizer subgroups FG_{n-1} , with seq.product $FG_n = FG_{n-1} C_n = C_n FG_{n-1}$. This construction holds in general, yielding coupled product recursion (3) also for $n > 4$:

$$(RFG) : \quad FG_n \cong FG_{n-1} \triangleright C_n \quad (4)$$

²<http://mathworld.wolfram.com/FiniteGroup.html>

COROLLARY 5.1 *Recursion (RFG) generates all full groups for $n > 2$.*

The structure of FG_n derives from that of FG_{n-1} : the defining r-congruence δ , specified by any stabilizer FG_{n-1} of FG_n , is extended by subgroup C_n as right-composing elements, functioning as last (rightmost) n -counter code-component, with $C_n \cong Z(+) \bmod n$.

Recall an even [odd] permutation is obtained from e by swapping an even [odd] number of state pairs. Their composition is like addition mod 2, thus $Z_2(+)$ with $odd = 1$, $even = 0$ which is isomorphic to a 2-cycle C_2 . Notice cyclic permutation C_n of n states is obtained by $n - 1$ pair swaps: $swap(i, i + 1)$, $swap(i + 1, i + 2)$ etc., hence its parity is that of $n - 1$.

Using the 2-part congruence of [odd, even] permutations in FG_{n-1} for coupling function γ : $FG_{n-1} \rightarrow aut(C_n)$, the odd permutations activate multiplier unit $-1 \in Z_n(\cdot)$ to yield permuted $[C_n]'$ for coupling purposes. This *odd/even* property of the elements of FG_{n-1} , respectively FG_n , can be represented by a first code component C_2 in a decomposition of FG_n , behaving as $Z(+)$ mod 2, with code values: $even = 0$, $odd = 1$.

Clearly each group with both odd and even permutations has this 2-part full congruence, hence with full image group C_2 as leading (first, leftmost) component in a cascade decomposition.

The order 60 of AG_5 has prime structure $|AG_5| = 2^2.3.5$ with C_3 and C_5 as even permutation cyclic subgroups of AG_5 . A 4-cycle permutation with closure C_4 (fixing one state) cannot occur in AG_5 because it is an odd permutation, but a subgroup of order 4 does exist (by Sylow's theorem), which must be $C_2 \times C_2$.

Now generate AG_5 by extending AG_4 (fig 4) with a factor group $d^* = C_5$, hence $AG_5 \cong C_5.AG_4 \cong AG_4.C_5$ where AG_4 functions as stabilizer AG_4' of state 4 in AG_5 (see fig 5). Such generation of AG_n with an alphabet of size $|A| = |AG_{n-1}| + n - 1$ yields a flat spectrum of height $|AG_{n-1}|$ and length n .

Note 5.1:

Orthogonal subgroups (intersecting pairwise only at e) in a sequential product commute.

For instance $C_5 AG_4' = AG_4' C_5 = AG_5$ despite non-commuting elements e.g: $ad \neq da$ (fig 5).

The alternating group AG_n of the $n!/2$ even permutations in FG_n is known to be a simple group for $n > 4$ [2]-p69, so without full congruence resp. normal subgroup [2]-p15. But AG_n ($n > 4$) does have subgroups, e.g. its Sylow p -subgroups, and as many r-congruences with corresponding coupled product (CP) as *permutation machine* of structure: $AG_n \cong AG_{n-1} \triangleright C_n$ if $n > 4$ is prime, and in general: with Sylow-compatible coupling(s) following Def 3.1.

Notice the orders of pair products of the four generators (table $|xy^*|$ in fig 5) do not depend on commutation: xy and yx have the same order. Because let xy have order m , so $(xy)^m \equiv x(yx)^{m-1}y \equiv e$ and no smaller m yields e . Then $(yx)^{m-1}y \equiv x^{-1} \implies (yx)^{m-1}yx \equiv e \implies (yx)^m \equiv e$ where again m is minimal, to prevent contradiction. In fact xy and yx have similar structure : $xys \equiv yx \pmod{Q}$ for some 'similarity' permutation s of state set Q .

The structure of AG_5 of order $|AG_4|.5 = 60$ extends that of AG_4 by a coupled product with C_5 having four symmetries (automorphisms): $C_4 \cong aut(C_5)$ into which AG_4 couples by Sylow component image $(C_2 \times C_2)/\gamma = C_2 = \{0, 1\}$ transforming $d \in C_5$ into $d' \equiv d$ if $(a, b)/\gamma = 0$, or $d' \equiv 4d \equiv -d \pmod{5}$ if $(a, b)/\gamma = 1$.

This yields the next cascade structure of AG_5 as a network of coupled prime-counters:

$$AG_5 = AG_4 \triangleright C_5 = C_3 \triangleright (C_2 \times C_2) \triangleright_{\gamma} C_5 \cong \{c, a, b, d\}^* \quad (5)$$

To show that (5) represents simple group $AG_5 = \{a, b, c, d\}^*$ as given in fig 5, notice the iteration classes c^* , a^* , b^* , d^* are by construction of proper order: 3, 2, 2, 5 respectively. It remains to

AG5: C5 * (-- AG4' --) d.AG4' d^2.AG4' d^3.AG4'																					
----d----*-abc-----+-----,-----,-----																					
0		1234		210<033210132	302	121033201	033	210121023	121	302302310											
1		2340		302 121033201	033	210121023	121	302302310	444	444444444											
2		3401		033 210121023	121	302302310	444	444444444	210	033210132											
3		4012		121 302302310	444	444444444	210	033210132	302	121033201											
4		0123		444<444444444	210	033210132	302	121033201	033	210121023											
		-C5-	CCC																		
		d*	223 e	da								ad									
		d^4.AG4'											xy* c a b d								
--+-----+-----+-----+-----+-----+-----																					
0		444	444444444	3	3	3	2	2	1	3	3	2	0	1	2	c		-	3	3	5
1		210	033210132	2	2	1	0	0	3	4	0	1	3	3	3	a		3	-	2	5
2		302	121033201	1	1	0	1	1	2	1	1	4	2	4	1	b		3	2	-	3
3		033	210121023	0	0	2	3	3	0	2	4	3	4	2	4	d		5	5	3	-
4		121	302302310	4	4	4	4	4	4	0	2	0	1	0	0	orders of					
												<--- in AG4' --->					pair products				

Figure 5: Alternating group $AG_5 = AG_4$ extended by C_5 (60 even permutations)

verify the four generators have a 4-code and coupling such that their pairwise compositions are isomorphic to those in fig 5 as follows.

The four generators and their iterations have the next 4-codes, in network sequence as given in (5) , where $c^3 \equiv a^2 \equiv b^2 \equiv d^5 \equiv e \pmod{AG_5}$ with code $[0,0,0,0]$:

$$\begin{aligned}
[c] &= [1, 0, 0, 0] ; [a] = [0, 1, 0, 0] ; [b] = [0, 0, 1, 0] ; [d] = [0, 0, 0, 1] \\
[c^2] &= [2, 0, 0, 0] ; [a^2] = [0, 0, 0, 0] ; [b^2] = [0, 0, 0, 0] ; [d^2] = [0, 0, 0, 2] \\
[c^3] &= [0, 0, 0, 0] ; [d^3] = [0, 0, 0, 3] ; [d^4] = [0, 0, 0, 4] ; [d^5] = [0, 0, 0, 0]
\end{aligned}$$

The generators c, a, b of stabilizer AG_4' and their pair products need not be verified since $AG_4 \cong AG_4'$. Only the products cd, ad, bd with the new generator d need be compared with those of their coded versions: $[xd] = [x] \triangleright_\gamma [d]$ with $x \in \{c, a, b\}$, using coupled product with mapping $(C_2 \times C_2)/\gamma = C_2 \longrightarrow \text{aut}(C_5)$.

In fact $cd = c e d = c a^2 d = ca ad$, so only the coupled code product $[a] \triangleright_\gamma [d]$ must yield the code $[ad]$ of ad and similarly $[b] \triangleright_\gamma [d] = [bd]$, as they do upon inspection.

The coupled product (of p -subgroups) for groups relates to the following properties of sub-semigroups and image semigroups in general.

LEMMA 5.1 For any sub-semigroup : $T \subset S \implies \text{deg}(T) \leq \text{deg}(S)$

LEMMA 5.2 Any image semigroup : $U \cong S/\gamma \implies \text{dim}(U) \leq \text{dim}(S)$

PROOF. Any subsemigroup T of a semigroup S_n with $\text{deg}(S) = n$ states can also be represented over at most n states, since T is a closed subset of the n -state transforms representing S . Similarly the dimension (the minimal number of generators) of an image semigroup U of S is at most $\text{dim}(S)$, since U is obtained by equivalencing elements in S , which cannot increase its dimension. \square

So any subgroup of FG_n can be represented by at most n states.

And conversely, any group H with $\deg(H) = n$ is a subgroup of FG_n .

For groups: the coupled structure of $H \subset G$ as subgroup follows from that of G because subgroup order $|H|$ is known to divide group order $|G|$ (Lagrange's theorem [2]-p11). So the prime structure of $|H|$ derives from that of $|G|$ by reducing one or more exponents of its prime divisors.

COROLLARY 5.2 *For subgroup $H \subset G$ (finite) :*

The compatible ordering of the Sylow components of H ,

viz. its 'coupling structure', is covered by that of G .

From $AG_n \subset FG_n$ follows that the coupling structure of alternating group AG_n is similar to that of FG_n , yielding a loopfree coupled network of compatibly ordered Sylow components (thm 5.1). Regarding the loopfree decomposition of a non-cyclic [$\dim(G) > 1$] finite group G the property of being a 'simple group' is irrelevant.

The *odd/even* full congruence of FG_5 yields image C_2 and its Sylow component of order 2^3 contains odd permutations of order 4, since $C_4 \subset FG_5$. So AG_5 (fig 5) can be expanded to FG_5 by replacing for instance a of order 2 by an odd permutation f of order 4, such as $f = \sqrt{a}$ (thus $f^2 \equiv a$) or f^{-1} .

References

1. G.Birkhoff, T.Bartee: *Modern Applied Algebra*, McGraw-Hill (1970)
2. D.J.Robinson: *A Course in the Theory of Groups*, Graduate Texts in Maths nr.80, Springer Verlag (1982)
3. A.Suschkevitsch: *Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit*, Math.Ann.99, 30-50 (1928)
4. A.H.Clifford, G.B.Preston: *The Algebraic Theory of Semigroups*, AMS Survey nr.7 (vol I) appx.A, 207-208 (1961)
5. J.Hartmanis, E.Stearns: *Algebraic Structure of Sequential Machines*, McGraw-Hill, Englewood Cliffs, NJ (1970)
6. K.B.Krohn, J.L.Rhodes: "Algebraic Theory of Machines", Part I, *Tr.AMS* 116, 450-464 (1965)
7. A.Ginzburg: "Algebraic Theory of Automata", Acad. Press, NY (1968)
8. N.F.Benschop: *Semigroups of constant rank, and the five basic state machine types*, IFIP workshop "Logic and Architecture Synthesis" Paris (1990)
<http://de.arxiv.org/pdf/math.GM/0103112>
9. — : "Associative Digital Network Theory" (Ch.3), Springer Verlag (due Apr.2009)