REPRESENTATION OF GROUPS BY GENERALIZED NORMAL MULTIPLICATION TABLES

A. GINZBURG*

Introduction. G will denote a finite (or infinite) group of order n. In a normal multiplication table (n.m.t.) of G **(7, 8, 9, 12)** all entries in one diagonal are equal to e (the identity of G), and if the entry on the intersection of the ith column and jth row is $g_{i,j} \in G$, then

$$g_{i,j}\, g_{j,k} = g_{i,k}, \qquad g_{j,i} = g_{i,j}^{-1}.$$

The following is a n.m.t. of $Z_6 = \{0, 1, 2, 3, 4, 5\}$:

f	5	4	3	2	1	0
e	4	3	2	1	0	5
d	3	2	1	0	5	4
c	2	1	0	5	4	3
b	1	0	5	4	3	2
a	0	5	4	3	2	1
	a	b	c	d	e	f

Remark. The cyclic groups Z_n will always be written in additive notation.

The table is uniquely defined by every one of its columns, in particular by the first. Indeed,

$$g_{i,j} = g_{i,1}\, g_{1,j} = g_{1,i}^{-1}\, g_{1,j}.$$

The associativity ensures that this construction leads to a n.m.t. of G. If every $g \in G$ appears in the first column, the same is true for every other column (and row). Every multiplication ab $(a, b \in G)$ can be done n times in such a table.

By deletion of some columns and of the corresponding rows (i.e., columns and rows intersecting on the diagonal consisting of e's), one obtains a m.t. having all the above properties, except for the last one. However, the table

---

Received April 5, 1966. This paper is mainly contained in a doctoral thesis done under the guidance of Professor Dov Tamari, to whom the author wishes to express his great indebtedness. The thesis was presented to the Technion, Israel Institute of Technology, Haifa, Israel in 1959.

*On leave from Technion, Israel Institute of Technology, Haifa, Israel.

(9) obtained from the n.m.t. of Z_6 by deleting the d and f columns and rows, i.e.

e	4	3	2	0
c	2	1	0	4
b	1	0	5	3
a	0	5	4	2
	a	b	c	e

shows that one can still arrive at a table in which every multiplication ab $(a, b \in G)$ is done at least once.

This paper deals with the representation of groups by such *generalized* (g.) n.m.t., which are particular cases of so-called quasi-regular partitions, and can also represent other binary systems **(2–5, 10, 11)**.

1. Generating columns.

Definition. A set $D \subseteq G$ with the property that for every $a, b \in G$ there exist $d_i, d_j, d_k \in D$ such that

$$a = d_i^{-1} d_j, \qquad b = d_i^{-1} d_k \tag{1}$$

is called a *generating column* (g.c.) of G.

THEOREM 1. *Every g.c. D including e can serve as the first column in a g.n.m.t. of G, and conversely, the set of elements in the first column of a g.n.m.t. of G is a g.c. of this group.*

Proof. A square table is constructed with the elements of D (in an arbitrary order, except for $g_{1,1} = e$) as its first column. Set

$$g_{1,i} = d_i \in D, \qquad g_{i,j} = d_i^{-1} d_j.$$

Then $g_{i,i} = e$ for every i, $g_{i,1} = d_i^{-1}$, the associativity ensures that

$$g_{i,j}\, g_{j,k} = g_{i,k},$$

and it remains to show that every multiplication of two elements in G is done.

Let $ac = b$ be an arbitrary product in G. By (1)

$$\exists d_i, d_j, d_k \in D\colon\ a = d_i^{-1} d_j,\ b = d_i^{-1} d_k.$$

But

$$g_{j,k} = g_{j,1}\, g_{1,k} = d_j^{-1} d_k = (d_i^{-1} d_j)^{-1} (d_i^{-1} d_k) = a^{-1} b = c.$$

Hence, $g_{i,j} = a$, $g_{j,k} = c$, and the multiplication ac is done in the constructed table, which is thus a g.n.m.t. of G.

Conversely, let D be the set of elements of the first column in a given g.n.m.t. of G. For every $a, b \in G$ there exists a $c \in G$ such that $ac = b$. Hence in the g.n.m.t. one has the configuration:

$$g_{i,j} = a, \qquad g_{j,k} = c, \qquad g_{i,k} = g_{i,j}\, g_{j,k} = ac = b.$$

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

If, as before, $d_i = g_{1,i}$ for every i, then

$$a = g_{i,j} = d_i^{-1} d_j, \qquad b = g_{i,k} = d_i^{-1} d_k,$$

i.e., (1) is satisfied and D is a g.c. of G.

It follows from the proof that all products exist in the quadratic table (i.e., it is a g.n.m.t.) if and only if every pair $a, b \in G$ appears at least once in a common column of this table. This relation will be denoted by $a * b$ and called the *check* between a and b. It is symmetric and reflexive (every $a \in G$ appears in the table) but not transitive.

2. Some properties of generating columns.

LEMMA 1. *D and $D_1 = aDb$ $(a, b \in G)$ are simultaneously g.c. of G. This relation between the g.c. is an equivalence.*

Proof. If D is a g.c. of G, then:

$$(\forall g_1, g_2 \in G)(\exists d, d_1, d_2 \in D)\colon bg_1 b^{-1} = d^{-1} d_1,\ bg_2 b^{-1} = d^{-1} d_2,$$
$$g_1 = (adb)^{-1}(ad_1 b), \qquad g_2 = (adb)^{-1}(ad_2 b),$$

i.e., D_1 is also a g.c.

COROLLARY. *Every column of a g.n.m.t. of G is a g.c. of G, and all these g.c.'s are equivalent.*

D will be called an *irreducible* g.c. of G if no proper subset of D is a g.c. of G. It is easy to see that irreducibility is preserved under the above equivalence transformation of the g.c.

If $\phi\colon G \to G'$ is a homomorphism of G onto G', then $D\phi$ will be a g.c. of G'; but irreducibility is not invariant under homomorphism. For example, $D_1 = \{0, 1, 2, 4, 5, 8, 10\}$ and $D_2 = \{0, 1, 2, 4, 6, 7, 10\}$ are two irreducible g.c. of Z_{12}. Now, let ϕ be the homomorphism of Z_{12} onto Z_6. $D_1\phi = \{0, 1, 2, 4, 5\}$, $D_2\phi = \{0, 1, 2, 4\}$ (in Z_6). $D_1\phi$ is reducible, $D_2\phi$ is not. Moreover, $D_3 = D_2 \cup \{8\}$ is reducible (in Z_{12}), but $D_3\phi$ is not (in Z_6).

Definition. D_A is a set of elements of G, such that

$$(\forall a, b \in A)(\exists d, d_1, d_2 \in D_A)\colon a = d^{-1} d_1,\ b = d^{-1} d_2.$$

$D_G = D$.

PROPOSITION 1. *Let H be a subgroup of G and A a set of representatives, one from every right coset of H in G (e is taken from H). Then $D_H A$ is a g.c. of G.*

Proof. For every $g_1, g_2 \in G$, there exist $a_1, a_2 \in A$ and $h_1, h_2 \in H$ such that

$$g_1 = h_1 a_1, \qquad g_2 = h_2 a_2, \qquad (\exists d, d_1, d_2 \in D_H)\colon h_1 = d^{-1} d_1,\ h_2 = d^{-1} d_2.$$

Hence

$$g_1 = h_1 a_1 = d^{-1}(d_1 a_1), \qquad g_2 = h_2 a_2 = d^{-1}(d_2 a_2),$$

and since $d, d_1 a_1, d_2 a_2 \in D_H A$ this set is a g.c. of G.

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

PROPOSITION 2. *Let H be a normal subgroup of G, $G' = G/H = G\phi$ and $D' = D_{G'}$. Let C be any set of representatives of the cosets of H in G corresponding to the elements of D'. Then for every D_H the set $D_H C$ is a g.c. of G.*

Proof.

$$(\forall\, g_1, g_2 \in G)(\exists\, a_1, a_2 \in G)\colon g_1 \in a_1 H,\ g_2 \in a_2 H,$$
$$(\exists\, d', d_1', d_2' \in D')\colon a_1\phi = a_1' = d'^{-1} d_1',\ a_2\phi = a_2' = d'^{-1} d_2'.$$

Let c, c_1, c_2 be the elements of $C \subseteq G$ representing $d', d_1', d_2' \in D' \subseteq G'$ respectively. Then: $c^{-1} c_1 = a_3 \equiv a_1 \pmod H$, $c^{-1} c_2 = a_4 \equiv a_2 \pmod H$. There exist $h_1, h_2 \in H$, such that $g_1 = a_3 h_1$, $g_2 = a_4 h_2$. H is normal in G; hence

$$(\exists\, h_3, h_4 \in H)\colon h_3 c_1 = c_1 h_1,\ h_4 c_2 = c_2 h_2.$$

By definition of D_H:

$$(\exists\, d_i, d_j, d_k \in D_H)\colon h_3 = d_i^{-1} d_j,\ h_4 = d_i^{-1} d_k.$$

Thus:

$$(d_i c)^{-1} d_j c_1 = c^{-1} d_i^{-1} d_j c_1 = c^{-1} h_3 c_1 = c^{-1} c_1 h_1 = a_3 h_1 = g_1,$$
$$(d_i c)^{-1} d_k c_2 = c^{-1} d_i^{-1} d_k c_2 = c^{-1} h_4 c_2 = c^{-1} c_2 h_2 = a_4 h_2 = g_2,$$

i.e., $D_H C$ provides the check $g_1 * g_2$.

The following observation is of a somewhat different nature:

THEOREM 2. *Let $\{D_i\}$ $(i = 1, 2, \ldots)$ be a sequence of subsets of a group G such that:*

$$D_1 = D_G = D, \qquad D_2 = D_{D_1}, \ldots, \qquad D_k = D_{D_{k-1}}, \ldots.$$

For every k and every $g \in G$ there exist $c_1, c_2 \in D_k$ such that $c_1^{-1} c_2 = g$.

Proof. For $k = 1$ the conclusion is true by definition. Assume that it is satisfied for $k - 1$, i.e., that

$$(\exists\, b_1, b_2 \in D_{k-1})\colon b_1^{-1} b_2 = g.$$

Then

$$D_k = D_{D_{k-1}} \Rightarrow (\exists\, c, c_1, c_2 \in D_k)\colon c^{-1}c_1 = b_1,\ c^{-1}c_2 = b_2$$
$$\Rightarrow g = b_1^{-1}b_2 = (c^{-1}c_1)^{-1}(c^{-1}c_2) = c_1^{-1}c_2.$$

The theorem is proved by induction.

COROLLARY. *In a finite G of order n every D_k in the sequence of Theorem 2 contains at least $[n^{\frac{1}{2}} + 1]$ elements.*

3. Independent checks. The following part of a g.n.m.t.

g_2	$g_1^{-1}g_2$	e
g_1	e	$g_2^{-1}g_1$
e	g_1^{-1}	g_2^{-1}

shows that the checks

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

(2) $$g_1 * g_2, \qquad g_1^{-1} * g_1^{-1} g_2, \qquad g_2^{-1} * g_2^{-1} g_1$$

imply each other. They will be called *dependent checks.*

LEMMA 2. *Two of the three checks in* (2) *are identical if and only if the elements* e, g_1, g_2 *form a subgroup of* G. *Then all three checks in* (2) *are identical.*

Proof. $g_1^2 = g_2$, $g_1^3 = e \Rightarrow g_1^{-1} = g_2$, $g_1^{-1} g_2 = g_1$, $g_2^{-1} = g_1$, $g_2^{-1} g_1 = g_2$, and the three checks in (2) coincide.

Conversely, assume that they coincide; then

$$g_1^{-1} \neq g_2^{-1}, \qquad g_1 \neq g_2^{-1} g_1, \qquad g_2 \neq g_1^{-1} g_2,$$

$$g_1 = g_1^{-1} g_2, \qquad g_2 = g_1^{-1} \Rightarrow g_1^2 = g_2, \qquad g_1^3 = g_2 g_1 = g_1^{-1} g_1 = e.$$

The case $g_1 = g_2^{-1}$, $g_2 = g_2^{-1} g_1$ is analogous.

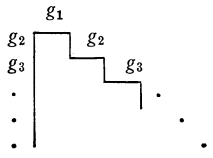
$$g_1^{-1} = g_2^{-1} g_1, \quad g_2^{-1} = g_1^{-1} g_2 \Rightarrow g_1^2 = g_2, \quad g_1^3 = g_1 g_2 = g_1 g_1 g_2^{-1} = g_2 g_2^{-1} = e.$$

For the $\frac{1}{2}(n-1)(n-2)$ checks in G of order n ($g * g$ and $g * e (g \in G)$ excluded) one has the following corollary.

COROLLARY. *If* $n \not\equiv 0 \pmod 3$, *the number of "independent" triples of checks is* $\frac{1}{6}(n-1)(n-2)$. *If* $n \equiv 0 \pmod 3$ *and there are* m *subgroups of order* 3 *in* G, *the number of independent triples of checks is*

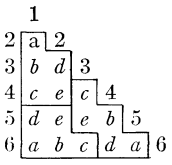
$$\tfrac{1}{3}[\tfrac{1}{2}(n-1)(n-2) - m] + m = \tfrac{1}{6}(n-1)(n-2) + \tfrac{2}{3}m.$$

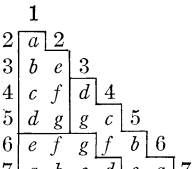
4. Table of checks. The checks can be recorded in a triangular table

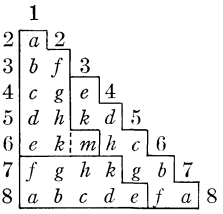


To every set of representatives of the above triples of checks (further: *a complete set of independent checks*) there corresponds a "part" of the table. For Z_n a convenient decomposition of the table of checks into such parts is exhibited by the following examples:

$n = 7 \equiv 1 \pmod 3$ $\qquad$ $n = 8 \equiv 2 \pmod 3$ $\qquad$ $n = 9 \equiv 0 \pmod 3$







This can be generalized as follows.

PROPOSITION 3. *For Z_n with $n \not\equiv 0 \pmod 3$ one of the parts consisting of independent checks, in the table of checks enumerated in the natural order, can be delimited by the row $j = [\frac{2}{3}n]$ and the column $i = [\frac{1}{3}n]$. If $n \equiv 0 \pmod 3$ such a part will be delimited by the row $j = \frac{2}{3}n$ and the column $i = \frac{1}{3}n - 1$. In both cases the row and column mentioned are included. For $n \equiv 0 \pmod 3$ $\frac{2}{3}n * \frac{1}{3}n$ also belongs to the above.*

LEMMA 3. *Let H be a normal subgroup of G, and assume that G/H has no subgroup of order 3. If $a, b, a^{-1}b \notin H$ $(a, b \in G)$, then no three cosets among*

$$aH, \quad bH, \quad a^{-1}H, \quad b^{-1}H, \quad a^{-1}bH, \quad b^{-1}aH$$

are equal. All checks

$$aH * bH = \{ah_i * bh_j\}_{h_i, h_j \in H}$$

are independent and imply that

$$a^{-1}H * a^{-1}bH \quad \text{and} \quad b^{-1}H * b^{-1}aH.$$

Proof. $aH \cap bH = \emptyset$. Hence all checks $ah_i * bh_j (h_i, h_j \in H)$ are different and imply that

$$h_i^{-1}a^{-1} * h_i^{-1}a^{-1}bh_j = a^{-1}bh_k, \qquad h_j^{-1}b^{-1} * h_j^{-1}b^{-1}ah_i = b^{-1}ah_m.$$

All these checks can be arranged as follows:

$$\begin{array}{ll} & (1')\ aH * bH\ (2'), \\ (3) & (3')\ a^{-1}bH * a^{-1}H\ (4'), \\ & (5')\ b^{-1}H * b^{-1}aH\ (6'). \\ & (1') \neq (2'). \end{array}$$

One has also:

$$\begin{aligned} &b^{-1}aa^{-1} = b^{-1} \notin H \Rightarrow (3') \neq (4'), \\ &bb^{-1}a = a \notin H \Rightarrow (5') \neq (6'), \\ &a^{-1}bb^{-1} = a^{-1} \notin H \Rightarrow (2') \neq (3'), \\ &a^{-1}b \notin H \Rightarrow (4') \neq (5'), \\ &b^{-1}aa^{-1} = b^{-1} \notin H \Rightarrow (6') \neq (1'). \end{aligned}$$

Three cosets can be equal only in one of the following two cases:

$$(1') = (3') = (5') \quad \text{and} \quad (2') = (4') = (6').$$

But

$$(1') = (5') \Leftrightarrow ab \in H \Leftrightarrow b^{-1}a^{-1} \in H \Leftrightarrow (2') = (4').$$

Hence it is impossible that three of the cosets will be equal and the other three pairwise different.

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

If three cosets are equal and at least two of the others are equal, then one has, among the checks of (3), identical checks. Let, for example, $ah_1 * bh_2$ and $a^{-1}bh_3 * a^{-1}h_4$ be identical. Denote by ϕ the natural homomorphism $\phi: G \to G/H$. Then, also, the checks $a\phi * b\phi$ and $(a\phi)^{-1}b\phi * (a\phi)^{-1}$ are identical. But this is impossible, because there is no subgroup of order 3 in G/H. The first part of the lemma is proved. The second follows immediately from the fact that all checks in (3) are different.

THEOREM 3. *A complete set of independent checks in a group G with a normal subgroup H and with G/H, which does not have a subgroup of order 3, is composed of:*

(1) *A complete set of independent checks in H.*

(2) *All checks in every one of the cosets of H (except H).*

(3) *All checks between some cosets of H: these are the pairs of cosets corresponding to pairs of elements of G/H in the checks of a complete set of independent checks of this group.*

Proof. The complete set of independent checks in H implies all checks in H.

$$ah_i * ah_j \ (a \notin H, h_i, h_j \in H)$$
$$\Rightarrow h_i^{-1}a^{-1} * h_i^{-1}a^{-1}ah_j = h_i^{-1}h_j \quad \text{and} \quad h_j^{-1}a^{-1} * h_j^{-1}a^{-1}ah_i = h_j^{-1}h_i.$$

Hence, $aH * aH \Rightarrow H * Ha^{-1}$, and when all checks in the cosets aH are completed, so are all checks between H and all its cosets. The checks among the elements of different cosets (except H) are treated in Lemma 3.

Remark. If G/H has subgroups of order 3, then Theorem 3 holds too, except that among the checks among the elements of two cosets of H in G, corresponding to the non-identity elements of such a subgroup, there will be dependent checks.

Example. Let G be the group

$$q_6 = \{e, A, A^2, A^3, A^4, A^5, B, C, D, E, F, K\}.$$

(The m.t. of q_6 is given in the Appendix.)

Let $H = \{e, A^3\}$. The cosets are

$$H, \quad AH = \{A, A^4\}, \quad A^2H = \{A^2, A^5\}, \quad BH = \{B, E\}, \quad CH = \{C, F\},$$
$$DH = \{D, K\}.$$

A complete set of independent checks in $G/H \cong S_3$ is, for example, (as elements of G/H one considers the cosets):

$$AH * A^2H, \quad AH * BH, \quad AH * CH, \quad AH * DH. \tag{4}$$

A complete set of independent checks in G is:

1. In H none.
2. In the cosets of H:

$$A * A^4, \quad A^2 * A^5, \quad B * E, \quad C * F, \quad D * K.$$

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

3. Between the elements of the cosets (4):

$$A * A^2, \quad A * A^5, \quad A^2 * A^4, \quad A^4 * A^5$$

(among these are three dependent checks; cf. the above remark),

$$\begin{array}{llll} A * B, & A * E, & A^4 * B, & A^4 * E, \\ A * C, & A * F, & A^4 * C, & A^4 * F, \\ A * D, & A * K, & A^4 * D, & A^4 * K. \end{array}$$

5. The minimum necessary length of a g.c. in a finite group.

Notation. n is the order of the group $G = \{g_1, g_2, \ldots, g_n = e\}$; r is the "length" of a g.c., i.e., the number of elements in a column of the corresponding g.n.m.t. of G; k_{g_i} is the number of times that $g_i \in G$ appears in the g.n.m.t.; $\bar{k} = min\,\{k_{g_i}\}\,(g_i \in G)$; and k_{g_i,g_j} is the number of checks $g_i * g_j$ in the g.n.m.t.

PROPOSITION 4. *For every G of order n it is necessary that*

$$r(r-1) \geqslant \bar{k}(n-1), \tag{5}$$

$$\bar{k}(r-2) \geqslant n-2. \tag{6}$$

Proof.

$$\sum_{i=1}^{n-1} k_{g_i} = r(r-1)$$

and (5) follows.

$$\sum_{j=1,\, j\neq i}^{n-1} k_{g_i,g_j} = k_{g_i}(r-2), \qquad i = 1, 2, \ldots, n-1.$$

The g.n.m.t. will be complete if every $k_{g_i,g_j} \geqslant 1$; hence (6) follows.

(5) and (6) imply that

$$r(r-1)(r-2) \geqslant (n-1)(n-2); \tag{7}$$

hence,

$$r \geqslant n^{\frac{2}{3}} \tag{8}$$

(equality holds for $n = 1$ only).

The least integer r satisfying (5) and (6) will be denoted by r_{mn} (the *minimum necessary* r).

For $n = 1, 2, \ldots, 15$ one obtains:

n:	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\bar{k}$:	1	2	3	2	2 or 3	2	2 or 3	2	2 or 3	2 or 3	3	2 or 3	3	3	3
r_{mn}:	1	2	3	3	4	4	5	5	6	6	6	7	7	7	7

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

6. Estimates for a sufficient r. r_{ms} (*minimal sufficient r*) will denote the length of a shortest possible g.c. of G. Clearly $r_{ms} \geqslant r_{mn}$. r_{mn} determined as above satisfies the obvious combinatorial requirements of the g.n.m.t. and depends only on the order of the group. By combinatorial arguments it was proved in **(1)** that for every group

$$r_{ms} < Cn^{\frac{2}{3}} \log^{\frac{1}{3}} n,$$

where C is a sufficiently large absolute constant.

In the Appendix smallest possible g.n.m.t. for all groups up to the order $n = 15$ are listed. One sees that different groups of the same order have different r_{ms}, and, moreover, for a particular group of a larger order r_{ms} can be smaller than for some group of a smaller order.

Remark. A g.c. of length r_{ms} is irreducible, but there can exist for the same group irreducible g.c. of different length; for example the following are two irreducible g.c. of Z_{15}:

$\{0, 1, 2, 4, 5, 8, 10\}$ of length 7 and $\{0, 1, 2, 3, 4, 5, 6, 7, 10\}$ of length 9.

The following lemma and proposition indicate some reasons why r_{ms} often exceeds r_{mn}.

LEMMA 4. *Let $\bar{D}$ be the first column in a still incomplete g.n.m.t. of a group G with centre Z. If for some $g \in Z$, $k_g \geqslant 2$ in this table, there will be necessarily repeated checks (i.e., checks appearing more than once) in the g.n.m.t., the first column of which is $\bar{D} \cup dg$, where $d \in \bar{D}$ and $dg \notin \bar{D}$.*

Proof. $k_g \geqslant 2 \Rightarrow \exists\, d_1, d_2, d_3, d_4 \in \bar{D}$: $g = d_1^{-1} d_2 = d_3^{-1} d_4$.

$$d_2^{-1}dg = gd_2^{-1}d = d_1^{-1}d_2\, d_2^{-1}d = d_1^{-1}d.$$
$$gd_2^{-1}d_4 = d_1^{-1}d_2\, d_2^{-1}d_4 = d_1^{-1}d_4.$$
$$gd_1^{-1}d_3 = d_1^{-1}d_3 g = d_1^{-1}d_3\, d_3^{-1}d_4 = d_1^{-1}d_4.$$

Hence $d_2^{-1}d_4 = d_1^{-1}d_3$ and the check $d_2^{-1}dg * d_2^{-1}d_4$, which appears after dg is added to $\bar{D}$, is identical with $d_1^{-1}d * d_1^{-1}d_3$ due to $\bar{D}$ only.

PROPOSITION 5. *Let Z be the centre of G, and $\bar{D}$ the first column in a still incomplete g.n.m.t. of G. If in this table*

$$k_{g_1}, k_{g_2} \geqslant 2 \ (g_1, g_2 \in Z) \quad \text{and} \quad k_{g_1, g_2} = 0,$$

then every completion of $\bar{D}$, giving the check $g_1 * g_2$, leads to repeated checks.

Proof. Inspect the different possibilities and use Lemma 4.

For any group deleting an element d from the g.c. D will reduce every k_{g_i, g_j} by at most 3, because the check $g_i * g_j$ can involve d only in the following three possibilities:

$$\left.\begin{aligned} g_i &= d^{-1}d_1 = d_3^{-1}d = d_5^{-1}d_6, \\ g_j &= d^{-1}d_2 = d_3^{-1}d_4 = d_5^{-1}d, \end{aligned}\right\} \quad (d_1, \ldots, d_6 \in D).$$

This results in the following theorem.

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

THEOREM 4. *In every group G of order n every subset of $[\frac{2}{3}n]+1$ or more elements is a g.c.*

By Proposition 2, if H is a normal subgroup of G, then

$$r_{D_G} \leqslant r_{D_H} \cdot r_{D_{(G/H)}}.$$

From this we get:

COROLLARY. *Let $G \supseteq G_1 \supseteq \ldots \supseteq G_{t-1} \supseteq G_t = e$ be a normal series of G. There exists a D_G such that*

$$r_{D_G} \leqslant [\tfrac{2}{3}n_1 + 1][\tfrac{2}{3}n_2 + 1] \ldots [\tfrac{2}{3}n_t + 1],$$

where $n_1, n_2, \ldots, n_t$ are the orders of the corresponding factors.

The following theorem provides a quite "economical" construction of a g.c. for an arbitrary finite cyclic group:

THEOREM 5. *Let $Z_n = \{0, 1, \ldots, n-1\}$ be the cyclic group of order n. Let x, y, k, t, m be non-negative integers and let*

$$q = ky + y - 1.$$

If the inequalities

$$q \leqslant x, \tag{9}$$

$$x + tq - y + 1 \geqslant [\tfrac{1}{3}n], \tag{10}$$

$$x + tq + (m-k)y \geqslant [\tfrac{2}{3}n] \tag{11}$$

are satisfied, then the

$$r = x + 1 + t(k + y - 1) + m \tag{12}$$

integers given by

$$a + h(x; a)[by + ch(k; b) + dqh(1; b) + eyh(t-1; d)\, h(k; b)h(y-1; c)], \tag{13}$$

where

$$\begin{aligned} a &= 0, 1, \ldots, x, \\ b &= 0, 1, \ldots, k, \\ c &= 0, 1, \ldots, y-1, \\ d &= 0, 1, \ldots, t-1, \\ e &= 0, 1, \ldots, m, \end{aligned}$$

constitute a generating column of Z_n. By suitable choice of the parameters x, y, k, t, m a D_{Z_n} can be obtained with

$$r < 6^{\frac{1}{3}} n^{\frac{2}{3}} \sim 1.8172 n^{\frac{2}{3}}. \tag{14}$$

In (13) $h(u; v)$ *is Heaviside's function defined by*

$$h(u; v) = \begin{cases} 0, & 0 \leqslant v < u, \\ 1, & u \leqslant v. \end{cases}$$

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

Proof. The proof consists of: (a) a proof of the completeness of the g.c. defined by (13); (b) a choice of parameters assuring (14).

(a) By Proposition 3 one has to show that $i * j$ for every two integers i, j satisfying $0 < i \leqslant [\frac{1}{3}n]$, $0 < j \leqslant [\frac{2}{3}n]$, $i < j$. α, β, $\gamma \in$ (13), such that $i = \alpha - \gamma$, $j = \beta - \gamma$ (i.e., $\alpha = i + \gamma$, $\beta = j + \gamma$) imply $i * j$.

The sequence (13) begins with $x + 1$ consecutive integers $0, 1, \ldots, x$. Then there are t "cycles" of $k + y - 1$ integers each; the first consists of the integers $x + y$, $x + 2y, \ldots, x + ky$, $x + ky + 1$, $x + ky + 2, \ldots$, $x + ky + y - 1$. Every such cycle closes with a "block" of y consecutive integers. (10) ensures that in one of these blocks the smallest integer is not smaller than $[\frac{1}{3}n]$.

After the last cycle the integers

$$x + tq + y, \quad x + tq + 2y, \ldots, \quad x + tq + my$$

appear in (13), and (11) provides that (13) has at least $k + 1$ integers not smaller than $[\frac{2}{3}n]$.

For $i > x$ consider the following two cases:

(1) i is not an element of a block in (13), or it is the first integer in such a block. Then $i = p + p_i$, where $p \in$ (13) and $0 \leqslant p_i < y$.

Let $i + uy - p_i = p + uy$ $(0 \leqslant u \leqslant k)$ be the first integer in the block closing the cycle containing p. For j $(> i)$ one has $j = s + s_j$, where $s \in$ (13) and $0 \leqslant s_j < y$.

If $y > p_i - s_j \geqslant 0$ one selects:

$$\gamma = uy - s_j,$$
$$\alpha = i + \gamma = i + uy - s_j = p + uy + (p_i - s_j),$$
$$\beta = j + \gamma = j + uy - s_j = s + s_j + uy - s_j = s + uy.$$

All these are in (13). Indeed, $\gamma = uy - s_j \leqslant ky - s_j < q \leqslant x$ (by (9)); α belongs to the block mentioned; $\beta = s + uy$ belongs to (13), because $s \in$ (13) (even if $s = [\frac{2}{3}n]$ this is true, since $u \leqslant k$).

If $y > s_j - p_i > 0$ put:

$$\gamma = (u + 1)y - s_j,$$
$$\alpha = i + \gamma = p + p_i + (u + 1)y - s_j = p + (u + 1)y - (s_j - p_i),$$
$$\beta = j + \gamma = s + s_j + (u + 1)y - s_j = s + (u + 1)y.$$

γ is in (13), because in this case $s_j \geqslant 1$; hence

$$\gamma \leqslant (k + 1)y - s_j \leqslant ky + y - 1 = q \leqslant x.$$

α is in the block beginning with $p + uy$, and β is, clearly, one of the integers of (13) (observe that in this case $s < [\frac{2}{3}n]$).

(2) i belongs to a block, but is not the first integer in it. By (10) i cannot belong to the block in the last cycle $(i \leqslant [\frac{1}{3}n])$. Hence, $i = x + dq + ky + c$, where $0 \leqslant d \leqslant t - 1$ and $1 \leqslant c \leqslant y - 1$. As before $j = s + s_j$ $(0 \leqslant s_j < y)$.

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

If $s_j = 0$ both i and j belong to (13) and $i * j$. If $s_j > c$ one takes:

$$\gamma = y - s_j,$$
$$\alpha = i + \gamma = x + dq + ky + c + y - s_j = x + dq + ky + y - (s_j - c),$$
$$\beta = j + \gamma = s + s_j + y - s_j = s + y.$$

γ and β belong to (13) and so does α, because it is still in the above block. If $0 < s_j \leqslant c$ $(c - s_j < y - 1)$ put:

$$\gamma = ky + y - s_j \leqslant q \leqslant x,$$
$$\alpha = i + \gamma = x + dq + ky + c + ky + y - s_j$$
$$= x + (d + 1)q + ky + c - s_j + 1 \leqslant x + (d + 1)q + ky + y - 1,$$
$$\beta = j + \gamma = s + s_j + ky + y - s_j = s + (k + 1)y.$$

γ and β are in (13) (for β note that $s_j > 0$); so is α, which is an integer in the block of the $(d + 1)$ cycle (it exists, because i is not in the last block).

The case $i \leqslant x$: If $i \leqslant x - y + 1$, then $i, i + 1, \ldots, i + y - 1$ belong to (13) and among $j, j + 1, \ldots, j + y - 1$ at least one integer must also belong to (13), because two numbers in (13) do not differ by more than y. If $x - y + 1 < i \leqslant x$, one has the above case (2), where i was an integer (not the first) in a block. The first part of the theorem is thus proved.

(b) The number of elements in (13) is $r = x + 1 + t(k + y - 1) + m$. One has to choose five non-negative integers x, y, k, t, m, such that for a given n the inequalities (9), (10), (11) will hold and r in (12) will be as small as possible. A routine computation, which will be omitted here, shows that in every case it is possible to make $r < 6^{\frac{1}{3}} n^{\frac{2}{3}}$.

Examples.

(1) $n = 60$, $y = 3$, $x = 5$, $k = 1$, $t = 4$, $m = 6$, $r = 24 \sim 1.57 \times 60^{\frac{2}{3}}$. The corresponding g.c. is :

0, 1, 2, 3, 4, 5, 8, 9, 10, 13, 14, 15, 18, 19, 20, 23, 24, 25, 28, 31, 34, 37, 40, 43.

(2) $n = 6000$, $y = 19$, $x = 180$, $k = 8$, $t = 11$, $m = 111$, $r = 578 \sim 1.75 \times 6000^{\frac{2}{3}}$.

The above construction can be improved very much in particular cases; for example, for Z_{40} one can construct a g.c. with $r = r_{mn} = 13 \sim 1.1 \times 40^{\frac{2}{3}}$.

Using Proposition 2 one obtains the following corollary.

COROLLARY. *For a G which is a direct product of t cyclic groups a g.c. can be constructed with $r < 6^{t/3} n^{\frac{2}{3}}$.*

7. Remarks about g.c. in infinite groups. For a g.c. in the infinite cyclic group Z_∞ one can use the construction of Theorem 5 with an infinite number of cycles. x and y can be increased arbitrarily (together with k), subject to the condition $q \leqslant x$. Thus, a g.c. of Z_∞ can be obtained with an arbitrarily small "density" of its elements.

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

For every infinite G, if D' (a finite set) is the first column of an incomplete g.n.m.t. of G, an $x \in G$ can always be found such that its addition to D' will produce only new independent triples of checks, all different. Indeed, such an element x has to satisfy only a finite number of conditions of the form $x \neq d_i d_k^{-1} d_j$ $(d_i, d_j, d_k \in D')$, and G is infinite.

It follows that if A is an arbitrary countable set of checks in an infinite G, an (incomplete) g.n.m.t. of G can be constructed such that all checks of A will appear in it, and the ratio of repeated independent triples of checks to the total number of checks in any finite quadratic segment of this table will be arbitrarily small.

Moreover, there exist particular infinite groups permitting construction of a g.n.m.t. with every independent triple of checks occurring exactly once.

Appendix. Minimal g.n.m.t. for all groups up to the order 15 inclusive.

Remark. The list of the groups mentioned and their notation is taken from **(6)**.

$n = 1$, $r_{ms} = r_{mn} = 1$ — Z_1:

0

$n = 2$, $r_{ms} = r_{mn} = 2$ — Z_2:

1	0
0	1

$n = 3$, $r_{ms} = r_{mn} = 3$ — Z_3:

2	1	0
1	0	2
0	2	1

$n = 4$, $r_{ms} = r_{mn} = 3$ — Z_4:

2	1	0
1	0	3
0	3	2

V_4:

C	B	e
A	e	B
e	A	C

$n = 5$, $r_{ms} = r_{mn} = 4$ — Z_5:

3	2	1	0
2	1	0	4
1	0	4	3
0	4	3	2

$\bar{k} = 2$ cannot be otained when $r = 4$ (cf. the table in § 5).

$n = 6$, $r_{ms} = r_{mn} = 4$ — Z_6:

4	3	2	0
2	1	0	4
1	0	5	3
0	5	4	2

π_3:

D	C	B	e
A^2A		e	B
A	e	A^2	C
e	A^2A		D

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

The above g.n.m.t. (up to $n = 6$) appear in **(9)**.

$n = 7$, $r_{ms} = r_{mn} = 5$

Z_7:

4	3	2	1	0
3	2	1	0	6
2	1	0	6	5
1	0	6	5	4
0	6	5	4	3

$\bar{k} = 2$ cannot be obtained for $r = 5$.

$n = 8$, $r_{ms} = r_{mn} = 5$

Z_8:

6	5	4	2	0
4	3	2	0	6
2	1	0	6	4
1	0	7	5	3
0	7	6	4	2

$S_{2\times 2\times 2}$:

E	C	F	B	e
G	F	C	e	B
D	B	e	C	F
A	e	B	F	C
e	A	D	G	E

$S_{4\times 2}$:

E	D	C	B	e
A^3	A^2A	e		B
A^2A	e	A^3E		
A	e	A^3A^2D		
e	A^3A^2A	C		

δ_4:

E	D	C	B	e
A^3	A^2A	e		B
A^2A	e	A^3C		
A	e	A^3A^2D		
e	A^3A^2A	E		

q_4:

C	D	E	B	e
A^3	A^2A	e		D
A^2A	e	A^3C		
A	e	A^3A^2B		
e	A^3A^2A	E		

$n = 9$. There are two groups of order 9: Z_9 and $S_{3\times 3}$. The $r_{mn} = 6$. For the cyclic group Z_9 this is also the r_{ms}:

Z_9:

7	6	5	3	1	0
6	5	4	2	0	8
4	3	2	0	7	6
2	1	0	7	5	4
1	0	8	6	4	3
0	8	7	5	3	2

The second is the abelian group $Z_3 \times Z_3$. For it, $r = 6$ is not sufficient. Indeed, this group has four subgroups of order 3; thus, in the g.n.m.t. at least 12 checks of the form $a * a^2$ $(a^3 = e)$ must appear. If $r = 6$, one has only five entries different from e in every column, i.e., in every column there can be at most

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

two checks of the above form. If all of them have to be done, every column must contain two such checks.

Denote the elements of the group by e, A, A^2, B, B^2, C, C^2, D, D^2.

$$A^3 = B^3 = C^3 = D^3 = e, \quad AB = C, \quad AC = D, \quad AD = B.$$

By symmetry one can assume that the first column contains $A * A^2$ and $B * B^2$. The corresponding part of the g.n.m.t. is

6						e
5	B^2	C^2	D^2	B	e	
4	B	D	C	e	B^2	
3	A^2	A	e	C^2	D	
2	A	e	A^2	D^2	C	
1	e	A^2	A	B^2	B	
	1	2	3	4	5	6

and for $g_{5,6}$ only C^2 or D^2 can be chosen. In both cases the g.n.m.t. will not be complete.

For this group $r_{ms} = 7$.

$S_{3\times 3}$:

B^2	C^2	D^2	C	A	D	e
C	B	D	A^2	C^2	e	D^2
C^2	D^2	B^2	B	e	C	A^2
D	C	B	e	B^2	A	C^2
A^2	A	e	B^2	B	D^2	D
A	e	A^2	C^2	D	B^2	C
e	A^2	A	D^2	C	C^2	B

$n = 10$
$r_{ms} = r_{mn} = 6$

Z_{10}:

8	7	6	4	2	0
6	5	4	2	0	8
4	3	2	0	8	6
2	1	0	8	6	4
1	0	9	7	5	3
0	9	8	6	4	2

$\bar{k} = 2$

7	6	5	3	2	0
5	4	3	1	0	8
4	3	2	0	9	7
2	1	0	8	7	5
1	0	9	7	6	4
0	9	8	6	5	3

$\bar{k} = 3$

δ_5:

C	D	E	F	B	e
A^4	A^3	A^2	A	e	B
A^3	A^2	A	e	A^4	F
A^2	A	e	A^4	A^3	E
A	e	A^4	A^3	A^2	D
e	A^4	A^3	A^2	A	C

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

$n = 11$ Z_{11}:
$r_{ms} = r_{mn} = 6$

7	6	5	3	2	0
5	4	3	1	0	9
4	3	2	0	10	8
2	1	0	9	8	6
1	0	10	8	7	5
0	10	9	7	6	4

$n = 12$ Z_{12}:
$r_{ms} = r_{mn} = 7$

10	9	8	6	5	2	0
8	7	6	4	3	0	10
5	4	3	1	0	9	7
4	3	2	0	11	8	6
2	1	0	10	9	6	4
1	0	11	9	8	5	3
0	11	10	8	7	4	2

$S_{6\times 2}$:

G	F	E	D	C	B	e
A^5	A^4	A^3	A^2	A	e	B
A^4	A^3	A^2	A	e	A^5	G
A^3	A^2	A	e	A^5	A^4	F
A^2	A	e	A^5	A^4	A^3	E
A	e	A^5	A^4	A^3	A^2	D
e	A^5	A^4	A^3	A^2	A	C

δ_6:

G	F	E	D	C	B	e
A^5	A^4	A^3	A^2	A	e	B
A^4	A^3	A^2	A	e	A^5	C
A^3	A^2	A	e	A^5	A^4	D
A^2	A	e	A^5	A^4	A^3	E
A	e	A^5	A^4	A^3	A^2	F
e	A^5	A^4	A^3	A^2	A	G

q_6:

C	D	E	F	G	B	e
A^5	A^4	A^3	A^2	A	e	E
A^4	A^3	A^2	A	e	A^5	D
A^3	A^2	A	e	A^5	A^4	C
A^2	A	e	A^5	A^4	A^3	B
A	e	A^5	A^4	A^3	A^2	G
e	A^5	A^4	A^3	A^2	A	F

a_4:

M	G	H	A	K	L	e
L	F	E	G	B	e	M
F	L	K	D	e	B	H
D	H	G	e	F	E	A
C	B	e	E	H	G	K
A	e	B	K	M	D	E
e	A	C	F	D	M	L

$n = 13$ Z_{13}:
$r_{ms} = r_{mn} = 7$

9	8	7	5	4	2	0
7	6	5	3	2	0	11
5	4	3	1	0	11	9
4	3	2	0	12	10	8
2	1	0	11	10	8	6
1	0	12	10	9	7	5
0	12	11	9	8	6	4

https://doi.org/10.4153/CJM-1967-072-2 Published online by Cambridge University Press

$n = 14$, $r_{mn} = 7$. There are two groups of this order: Z_{14} and δ_7. For both $r = 7$ is not sufficient. For δ_7, for example, one argues as follows: there are seven elements or order 2. Every one of them must appear in the g.n.m.t. an even number of times. But for $r = 7$, $\bar{k} = 3$. Thus, every element of order 2 appears in the g.n.m.t. at least four times and together they occupy a total of at least 28 entries. Even if each of the other six elements (except the identity) appears in the g.n.m.t. exactly three times, there will be at least $28 + 18 = 46$ entries outside the diagonal, while in a 7×7 table there are only 42 such entries. The proof for Z_{14} is more complicated and will be omitted.

For both groups $r_{ms} = 8$.

Z_{14}:

9	8	7	6	4	3	1	0
8	7	6	5	3	2	0	13
6	5	4	3	1	0	12	11
5	4	3	2	0	13	11	10
3	2	1	0	12	11	9	8
2	1	0	13	11	10	8	7
1	0	13	12	10	9	7	6
0	13	12	11	9	8	6	5

δ_7:

B	H	G	F	E	A^4	A^2	e
D	C	B	H	G	A^2	e	A^5
F	E	D	C	B	e	A^5	A^3
A^4	A^3	A^2	A	e	B	G	E
A^3	A^2	A	e	A^6	C	H	F
A^2	A	e	A^6	A^5	D	B	G
A	e	A^6	A^5	A^4	E	C	H
e	A^6	A^5	A^4	A^3	F	D	B

$n = 15$
$r_{ms} = r_{mn} = 7$

Z_{15}:

10	9	8	6	5	2	0
8	7	6	4	3	0	13
5	4	3	1	0	12	10
4	3	2	0	14	11	9
2	1	0	13	12	9	7
1	0	14	12	11	8	6
0	14	13	11	10	7	5

References

1. P. Erdös and A. Ginzburg, *On a combinatorial problem in latin squares*, Publ. Math. Inst. Hungar. Acad. Sci., Ser. A, *8* (1963), 407–411.
2. A. Ginzburg, *Multiplicative systems as homomorphic images of square sets*, thesis, Technion, Israel Institute of Technology, Haifa, 1959.
3. ——— *Systèmes multiplicatifs de relations. Boucles quasiassociatives*, C. R. Acad. Sci. Paris, *250* (1960), 1413–1416.
4. ——— *A note on Cayley loops*, Can. J. Math., *16* (1964), 77–81.
5. A. Ginzburg and D. Tamari, *Representation of binary systems by families of binary relations*, submitted for publication.
6. B. Higman, *Applied group-theoretic and matrix methods* (Oxford, 1955).
7. D. Tamari, *Monoïdes préordonnés et chaînes de Malcev*, Bull. Soc. Math. France, *82* (1954), 53–96, and additional stencils with the original manuscript of this thesis.

8. ——— *Les images homomorphes des groupoïdes de Brandt et l'immersion des semi-groupes*, C. R. Acad. Sci. Paris, *229* (1949), 1291–1293.
9. ——— *Représentations isomorphes par de systèmes de relations. Systèmes associatifs*, C. R. Acad. Sci. Paris, *232* (1951), 1332–1334.
10. ——— "*Near groups*" *as generalized normal multiplication tables*, Not. Amer. Math. Soc., *7* (1960), 77.
11. D. Tamari and A. Ginzburg, *Representation of multiplicative systems by families of binary relations* (*I*), J. London Math. Soc., *37* (1962), 410–423.
12. H. J. Zassenhaus, *The theory of groups* (Chelsea, 1958).

Carnegie Institute of Technology,
Pittsburgh, Pennsylvania, U.S.A.