TPP Triples of Subsets in Finite Groups

Sandeep Murthy
Research Student, Mathematics,
(University of London)

(to start in Jan. 2012)

Outline

1. Motivation - Complexity of Matrix Multiplication
2. TPP Triples - Fundamentals
3. TPP Triples - Examples & Problems
4. GAP Programs for TPP Triples - Verification and Search
5. Complexity Applications - 3 x 3 and 4 x 4 Matrix Multiplication
6. Conclusion

Motivation - Complexity of Matrix Multiplication

* Matrix multiplication is a bilinear map

$$\phi_{l,m,n} : K^{l\times m} \times K^{m\times n} \longrightarrow K^{l\times n}$$

* Rank of matrix multiplication - measure of bilinear complexity

$$R\left(\phi_{l,m,n}\right) := \min\left\{ r \in \mathbb{N} \;\middle|\; \phi_{l,m,n} = \sum_{i=1}^{r} f_i^* \cdot g_i^* \cdot C_i;\ \forall_i\, f_i^* \in K^{l\times m*}, g_i^* \in K^{m\times n*}, C_i \in K^{l\times n} \right\}$$

* Trivial rank bounds (1)

$$A \text{ is } K\text{-algebra} \Longrightarrow (\mathrm{Dim}\ A) \leq R(A) \leq (\mathrm{Dim}\ A)^2$$

$$n^2 \leq R(K^{n\times n}) = R(\phi_{n,n,n}) \leq n^4$$

$$R(K^{n\times n}_{\mathrm{diag}}) = n$$

Motivation - Complexity of Matrix Multiplication

* Exponent of matrix multiplication measures asymptotic complexity

$$\omega(K) := \inf\left\{e > 0 \,\middle|\, R(\phi_{n,n,n}) = \mathcal{O}(n^e),\ n \longrightarrow \infty\right\}$$

* Standard matrix multiplication (MM) algorithm achieves exponent 3

$$2n^3 - n^2 \text{ total ops.} \ = n^3 \text{ multiplications } + (n^3 - n^2) \text{ additions, subtractions}$$

* Trivial exponent bounds $2 \leq \omega(K) \leq 3$

* Strassen's MM algorithm (1969) achieves exponent 2.81

Motivation - Complexity of Matrix Multiplication

* Strassen's general MM algorithm is recursive application of efficient 2 x 2 MM algorithm using 7 multiplications (not 8 as in standard algorithm) - uses 12.5% fewer operations {*, $+$, -}

* (Slightly less) trivial rank bounds (2) - $(lmn)^{\frac{\omega}{3}} \leq R(l,m,n) \leq lmn$

* H. Cohn & C. Umans (2003) - if a finite group G realises a TPP triple of subsets S,T,U of sizes l,m,n resp. then

$$R(l,m,n) \leq R(\mathbb{C}[G]) \leq \sum_{i=1}^{r} R(d_i) \leq \sum_{i=1}^{r} d_i^3$$

$$\omega(\mathbb{C}) \leq 3\frac{\log R(\mathbb{C}[G])}{\log(lmn)} \leq 3\frac{\log \sum_{i=1}^{r} d_i^3}{\log(lmn)}$$

Motivation - Complexity of Matrix Multiplication

* TPP triples - nontrivial rank bounds for n x n by n x n MM possible via a group G only if

$$G \text{ has TPP triple of type } \langle n, n, n \rangle \ \& \ R(\mathbb{C}[G]) < n^3$$

* TPP triples - best rank upper bounds for n x n by n x n MM possible via a group G only if

$$G \text{ has TPP triple of type } \langle n, n, n \rangle \ \& \ R(\mathbb{C}[G]) < \mathrm{B}(n)$$

* Quite useful are groups with character degrees $<= 2$

$$G \text{ has largest character degrees } \leq 2 \Longrightarrow R(\mathbb{C}[G]) = 2|G| - r = r_1 + 7r_2$$

TPP Triples - Fundamentals

* Equivalent definition of a TPP triple (S,T,U) in/of a group G

$$Q(S) \cap Q(T)Q(U) = Q(T) \cap Q(U) = \{1\} \qquad \forall\, X \subseteq G, \quad Q(X) := \{x'x^{-1} \mid x, x' \in X\}$$

* Invariance properties - (1) permutation invariance (trivial)

$$(S,T,U) \text{ TPP in } G \iff (\pi(S), \pi(T), \pi(U)) \text{ TPP in } G \qquad \forall \pi \in \mathrm{Sym}_3$$

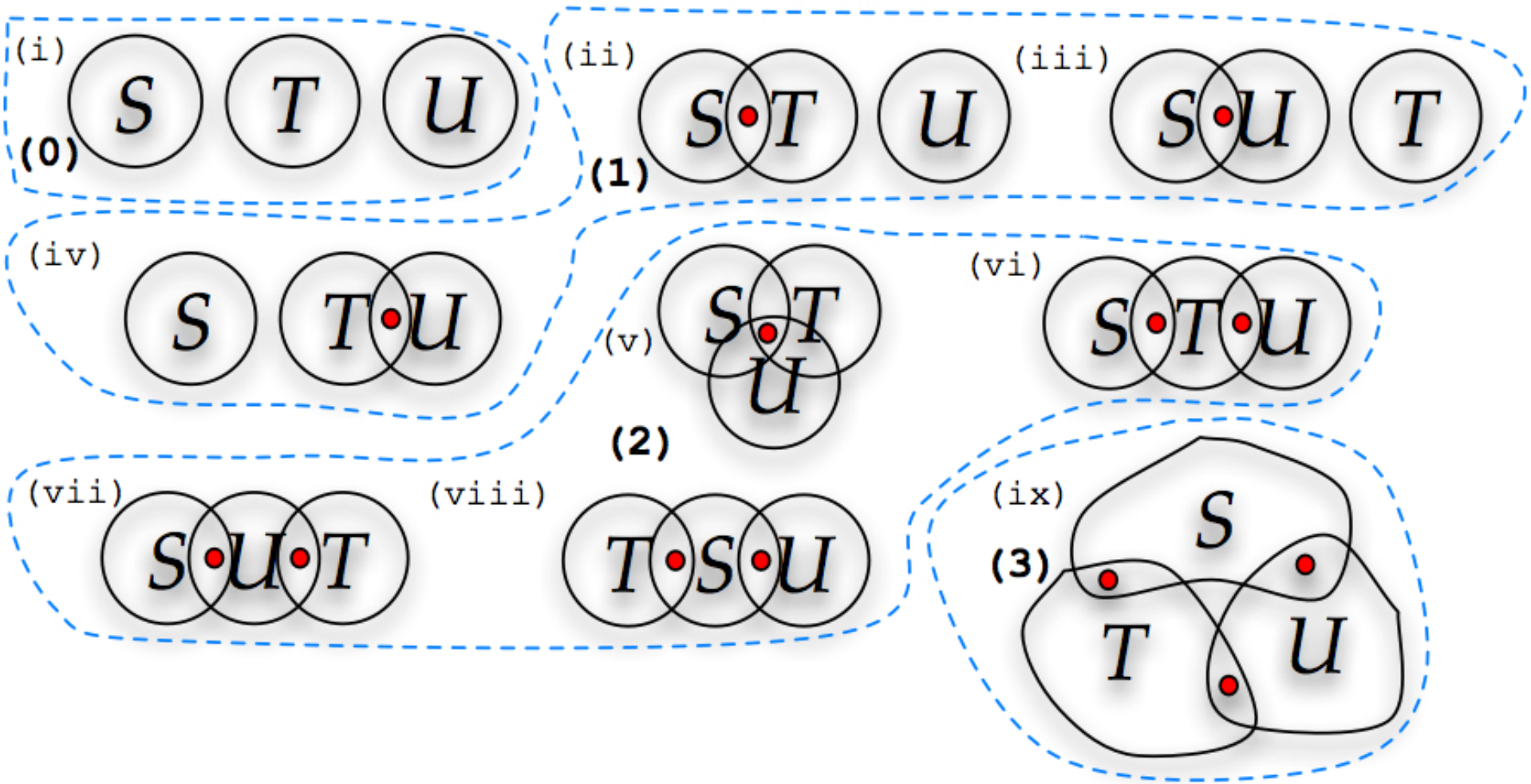
* Invariance properties - (2) translation invariance (nontrivial)

$$(S,T,U) \text{ TPP in } G \iff (wSx, wTy, wUz) \text{ TPP in } G \qquad \forall w, x, y, z \in G$$

* Can assume $1 \in S \cap T \cap U$ & $|S| \geq |T| \geq |U|$

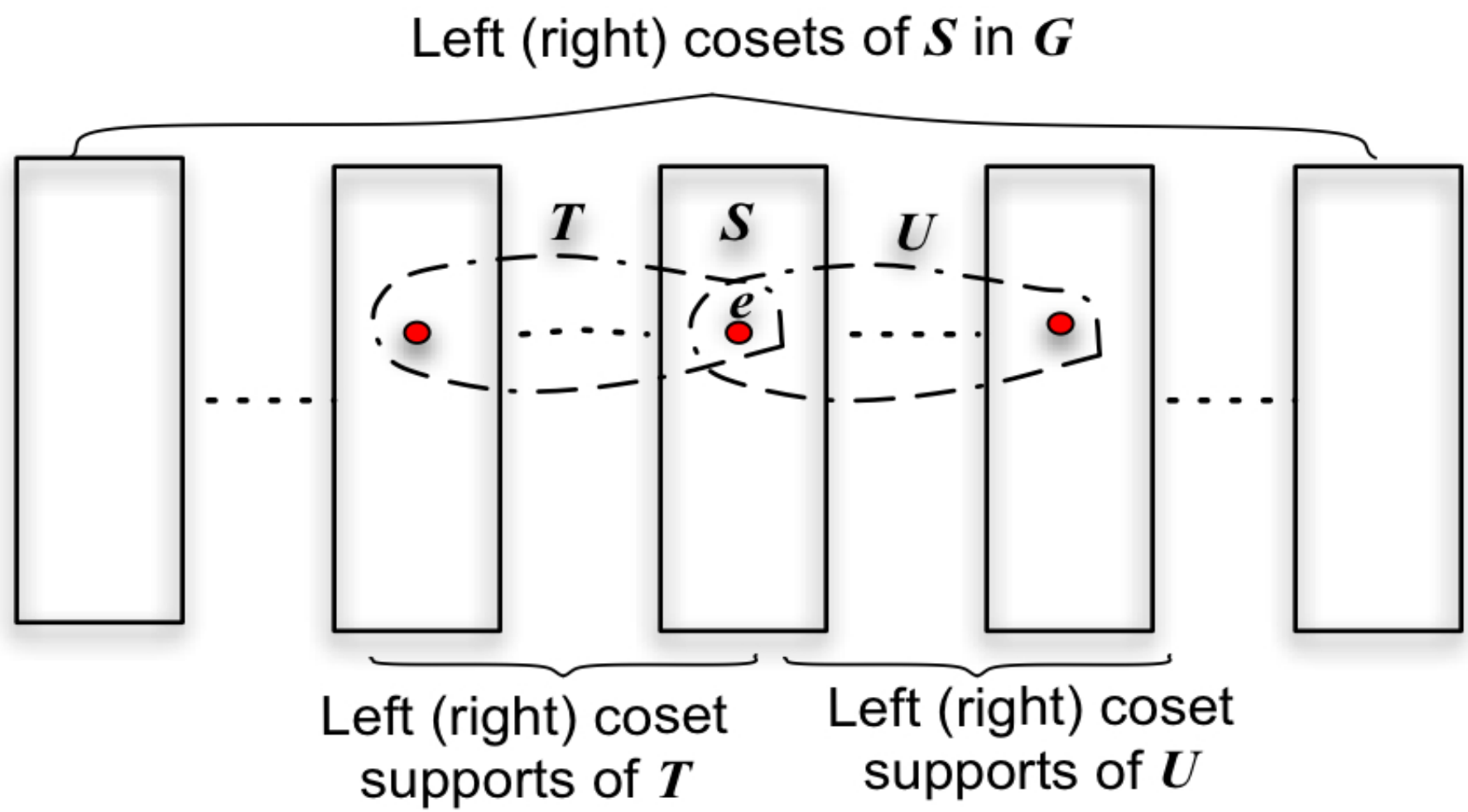
TPP Triples - Fundamentals

* What does a TPP triple (S,T,U) look like? (1) - in general



TPP Triples - Fundamentals

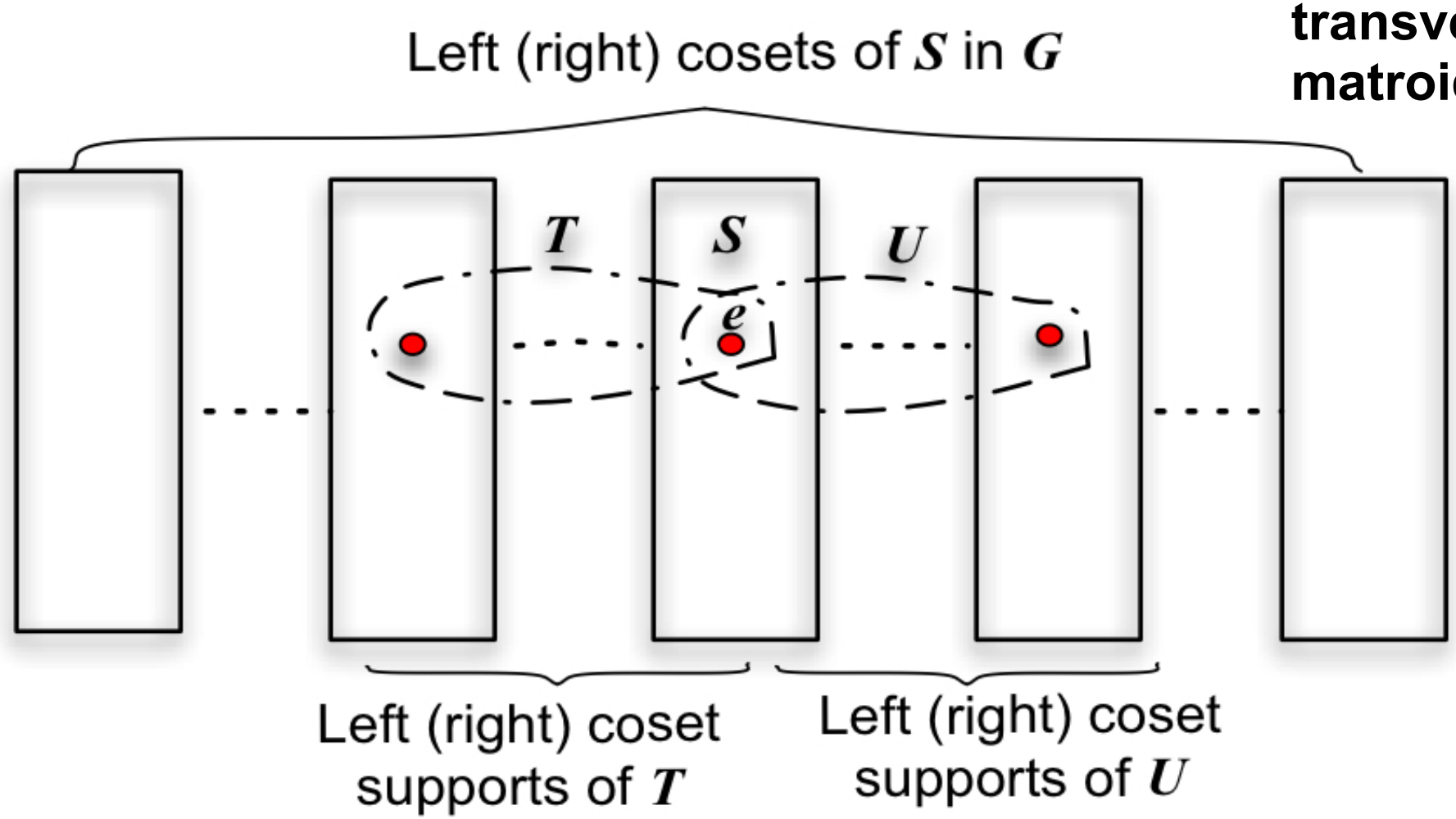
* What does a TPP triple (S,T,U) look like? (2) - when one member, say, S, is a subgroup



TPP Triples - Fundamentals

* What does a TPP triple (S,T,U) look like? (2) - when one member, say, S, is a subgroup

A special transversal matroid?



TPP Triples - Fundamentals

* Basic definitions & properties - TPP triple (S,T,U) of a group G

$$\text{type} := \langle |S|, |T|, |U| \rangle \qquad \text{size} := |S||T||U|$$

* Basic inequalities

$$|X^{-1}Y| = |X||Y|, \quad \forall \text{ distinct } X, Y \in \{S, T, U\}$$

$$|X|(|Y| + |Z| - 1) \leq |G|, \quad \forall \text{ distinct } X, Y, Z \in \{S, T, U\}$$

* 2nd inequality implies min. size of G to realise n x n matrix multiplication in $\mathrm{C}[G]$ is $2n^2 - n$

* Subgroup TPP triple satisfies $S \cap TU = T \cap U = 1, \quad (S, T, U \leq G)$

TPP Triples - Fundamentals

* Definitions - TPP Capacity of group G

$$\beta(G) := \max \left\{ |S||T||U| \;\middle|\; (S,T,U) \text{ is TPP in } G \right\}$$

* Definitions - Subgroup TPP Capacity of group G

$$\beta_0(G) := \max \left\{ |S||T||U| \;\middle|\; (S,T,U) \text{ is subgroup TPP triple of } G \right\}$$

* Trivial upper and lower bounds for TPP capacity, subgroup TPP capacity

$$|G| \leq \beta(G) < |G|^{\frac{3}{2}} \qquad |G| \leq \beta_0(G) \leq \beta(G)$$

* Fundamental theorem of TPP capacity for abelian groups

$$G \text{ is abelian } \Longrightarrow \beta(G) = |G|$$

TPP Triples - Fundamentals

* Parameter for measuring asymptotic efficiency of group-theoretic matrix multiplication

$$\omega(G) := 3\frac{\log R(\mathbb{C}[G])}{\log \beta(G)}$$

* A "good" group should satisfy

$$\omega(G) := 3\frac{\log R(\mathbb{C}[G])}{\log \beta(G)} \iff R(\mathbb{C}[G]) < \beta(G)$$

* Current best strict upper bound for exponent is 2.3755 (Coppersmith & Winograd, 1990)

* A (nonabelian) group G will give us a **new** / **best** exponent upper bound if $\omega(G) < 2.3755$

TPP Triples - Fundamentals

* Two basic results - (1) (S,T,U) is a subgroup TPP triple of G if and only if T & U are subtransversals for S in G with coset supports $\mathrm{supp}_S(T)$, $\mathrm{supp}_S(U)$ intersecting only in the trivial coset S

* Two basic results - (2) if a TPP triple (S,T,U) of G composed of two permuting subgroups, or a normal subgroup, then $|S||T||U| <= |G|$

* (2) suggests nonabelian groups with large numbers of large-order non-normal subgroups probably achieve large nontrivial TPP & subgroup TPP capacities

TPP Triples - Examples & Problems

* Dihedral groups $D_{2n} = \left\langle a, b \;\middle|\; a^n = b^2 = 1;\; bab = a^{-1} \right\rangle$- TPP capacity

$$\left(S_n = \left\{ a^{3k}, ba^{3k+1} \;\middle|\; 0 \le k < \frac{n-2}{3} \right\},\; T_n = \langle b \rangle, U_n = \langle ba^2 \rangle \right)$$

(Cohn & Umans, 2003)

$$\text{type } \left(\frac{|D_{2n}|}{3}, 2, 2 \right) \qquad \text{size } \frac{4}{3}|D_{2n}| = \frac{8n}{3}$$

$$\Longrightarrow \beta(D_{2n}) \ge \frac{4}{3}|D_{2n}|$$

* Subgroup TPP capacity

$$\text{largest subgroup TPP triples} = \begin{cases} \left(S_n = \langle a^3, ab \rangle, T_n = \langle b \rangle, U_n = \langle ba^2 \rangle \right), & 3 | n \\ \left(S_n = D_{2n}, T_n = \{1\}, U_n = \{1\} \right), & 3 \nmid n \end{cases}$$

$$\Longrightarrow \beta_0(D_{2n}) = \begin{cases} \frac{4}{3}|D_{2n}|, & n \text{ is a multiple of } 3 \\ D_{2n}, & n \text{ is not a multiple of } 3 \end{cases}$$

TPP Triples - Examples & Problems

* Symmetric groups Sym_n - Subgroup TPP capacity

$$\forall k \in [2..n-1]$$

$$\left(S_{n,k} = \mathrm{Stab}_n(k) = \mathrm{Sym}_{n-1},\ T_{n,k} = \langle (1\ 2 \cdots k) \rangle, U_{n,k} = \langle (k\ k+1 \cdots n) \rangle\right)$$

$$\text{type } ((n-1)!, k, n-k+1) \qquad \text{size } [k(n-k+1)](n-1)!$$

$$\Longrightarrow \beta(\mathrm{Sym}_n) \geq \beta_0(\mathrm{Sym}_n) > \frac{1}{4} n |\mathrm{Sym}_n| = \frac{1}{4} n^2 (n-1)!$$

TPP Triples - Examples & Problems

* Special linear groups $\mathrm{SL}(n,q)$ - Nontrivial-type subgroup TPP triples

$$(S_{n,q} = \{\text{upper unitriangulars}\}, T_{n,q} = \{\text{lower unitriangulars}\}, U_{n,q} = \{\text{diagonals}\})$$

$$\text{type } \left(q^{n(n-1)/2}, q^{n(n-1)/2}, (q-1)^{n-1}\right) \qquad \text{size } q^{n(n-1)}(q-1)^{n-1}$$

TPP Triples - Examples & Problems

* All (nonabelian) p-groups of orders p^3, p^4, and all (nonabelian) p-groups of order p^5 with abelian subgroups of index p have trivial subgroup TPP capacity!

Group order	***Largest Subgroup TPP triple type***	***Subgroup TPP capacity***
p^3	$<p,p,p>$	p^3
p^4	$<p^2,p,p>$	p^4
p^5	$<p^2,p^2,p>$	p^5

TPP Triples - Examples & Problems

* Estimating TPP capacity & subgroup TPP capacity as combinatorial optimisation problems -

maximise triple product $|S||T||U|$ *of subsets/subgroups* S,T,U *of a group* G *subject to subset/subgroup TPP conditions*

* Best known upper bound for TPP Capacity (P. M. Neumann, 2011)

* Conditional lower bounds for subgroup TPP capacity - (1) $4|G| / 3$ if G has a non-normal subgroup of index 3

* Conditional lower bounds for subgroup TPP capacity - (2) $3|G| / 2$ if G has a self-normalising subgroup of index 4

GAP Programs for TPP Triples

* TPP verification and search programs developed and implemented on the Groups, Algorithms, Programming (GAP) computer algebra system

* Joint work with Ivo Hedtke (Research Assistant, MLU Halle) - code and results can be found at

http://www2.informatik.unihalle.de/da/hedtke/tpp/algorithms.txt

http://www2.informatik.uni-halle.de/da/hedtke/tpp/resultsSUBSETS.html

http://www2.informatik.uni-halle.de/da/hedtke/tpp/resultsGROUPS.html

GAP Programs for TPP Triples

* Computed subgroup TPP capacities of all groups of order up to 1000 - approx. 48,000 different groups!

* Computed subset TPP capacity of all groups of order up to 32

http://www2.informatik.unihalle.de/da/hedtke/tpp/algorithms.txt

http://www2.informatik.uni-halle.de/da/hedtke/tpp/resultsSUBSETS.html

http://www2.informatik.uni-halle.de/da/hedtke/tpp/resultsGROUPS.html

* Preprint of TPP triples, algorithms, selected data, and conjectures to appear in a paper in Groups - Complexity - Cryptology (GCC) journal in 2012

GAP Programs for TPP Triples

* Current search programs are exponential in order of input groups

* Future aim is to develop a constructive algorithm for TPP triples that will construct a TPP triple of largest in a given group of a given type, using generators and presentation

http://www2.informatik.unihalle.de/da/hedtke/tpp/algorithms.txt

http://www2.informatik.uni-halle.de/da/hedtke/tpp/resultsSUBSETS.html

http://www2.informatik.uni-halle.de/da/hedtke/tpp/resultsGROUPS.html